www.informaticafacil.com.pt

INFORMÁTICA FÁCIL

N.º 83
bimestral
Informática | Internet | Multimédia | Jogos
Julho/Agosto/Setembro 2024

DEIXE DE USAR O GOOGLE MAPS

Saiba a razão e conheça as melhores alternativas!

LIVRE-SE DAS PASSWORDS ANTIGAS AGORA!

12345678
Pa55word
W!ndows
Admin123
Us3rname

Verifique se já foi pirateado e saiba como agir para não voltar a ser!

- Crie passwords impossíveis de piratear
- Mude já para passkeys
- Receba alertas por e-mail se as suas passwords forem pirateadas
- e muitos outros segredos!

ACELERE O SEU PORTÁTIL SEM GASTAR UM CÊNTIMO

PRÁTICA

- IMPEÇA OS SEUS VIZINHOS DE UTILIZAREM A SUA REDE WI-FI
- PARTILHE FICHEIROS ENTRE O SEU PC E O SEU TELEMÓVEL FACILMENTE

O WINDOWS INCLUI PROTEÇÃO INTEGRADA CONTRA SOFTWARE MALICIOSO. EIS COMO A ATIVAR

SUMÁRIO

LIVRE-SE DAS PASSWORDS ANTIGAS AGORA!
Com o roubo de palavras-passe a disparar, nunca foi tão importante livrar-se dos seus logins antigos e inseguros e começar a utilizar substitutos novos e invioláveis - incluindo passkeys. Aqui, explicamos o que deve fazer. **#04**

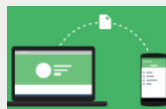
DEIXE DE USAR O GOOGLE MAPS
O Google Maps é a aplicação mais popular para explorar o mundo, mas nos últimos tempos tem vindo a decair. Neste artigo, explicamos o que correu mal e o que deve utilizar em vez dela. **#13**

ACELERE O SEU COMPUTADOR PORTÁTIL SEM GASTAR UM CÊNTIMO
Todos desejamos que nosso computador funcione de maneira plena, rápida e estável, mas isso nem sempre ocorre, especialmente com portáteis. Neste artigo, oferecemos algumas sugestões gratuitas que pode experimentar para melhorar o desempenho do seu PC. **#17**

O WINDOWS INCLUI PROTEÇÃO INTEGRADA CONTRA SOFTWARE MALICIOSO. EIS COMO A ATIVAR
Saiba como deve configurar o Windows Defender para evitar ser apanhado na rede do ransomware e outros programas maliciosos. **#22**

FREEWARE
- Uma das mais eficientes ferramentas de pesquisa de ficheiros e pastas

PRÁTICA

IMPEÇA OS SEUS VIZINHOS DE UTILIZAREM O SEU WI-FI
A não ser que viva numa área remota, o seu sinal Wi-Fi irá quase de certeza entrar na casa do seu vizinho. Desde que tenha definido uma palavra-passe forte, não deve ser fácil para os vizinhos "apanharem boleia" na sua rede de banda larga - mas pode ainda ser possível. Por isso, vale a pena verificar regularmente quais os dispositivos que estão ligados ao seu router para se familiarizar com os dispositivos que devem (e não devem) estar ligados. Aqui explicamos como fazer isso e bloquear quaisquer dispositivos não autorizados para impedir que descarreguem conteúdos ou acedam a sites duvidosos através da sua ligação. Estamos a utilizar um router Huawei OptiXstar (da Vodafone), pelo que as opções no seu router podem variar ligeiramente, mas devem ser muito semelhantes. **#26**

PARTILHE FICHEIROS ENTRE O SEU PC E O SEU TELEMÓVEL
Os serviços na nuvem, como o Google Drive e o iCloud, simplificam
a tarefa de partilhar ficheiros entre o telemóvel e o computador. O problema é que, quando se partilha desta forma, é fácil acabar com ficheiros soltos a ocupar o armazenamento na nuvem depois de concluída a transferência. Isto desperdiça espaço em disco, pelo que, a não ser que faça uma limpeza, poderá um dia ter de pagar por armazenamento adicional. Em alternativa, pode utilizar o LocalSend, que, em vez de encaminhar ficheiros através da nuvem, os envia diretamente através da sua rede. É totalmente gratuito, sem restrições. **#29**

Estatuto Editorial

Informática Fácil orienta a sua actividade pelos princípios da Declaração Universal dos Direitos
do Homem e no respeito pelos direitos, liberdade e garantias asseguradas pela Constituição da República Portuguesa.

Informática Fácil rege a sua actuação pelo respeito dos princípios deontológicos e da ética profissional dos jornalistas, assim como pela boa fé dos leitores.

Informática Fácil é um jornal mensal de notícias e ajudas na área das novas tecnologias, orientada por critérios de rigor, de isenção, de objetividade e criatividade editorial, sem qualquer dependência de ordem ideológica, religiosa, política ou económica.

Informática Fácil assegurará o pluralismo na informação que publica.

5Informática Fácil considera que a existência de uma opinião pública informada e actica é condição fundamental de democracia.

Informática Fácil pretende contribuir para a informação do público, garantindo aos cidadãos o direito de informar, de se informar e de ser informado, sem quaisquer impedimentos ou discriminações.

Informática Fácil actuará no estrito respeito pela dignidade dos trabalhadores, conduzindo-
se estes de acordo com os princípios estatutários, deontológicos, legais e constitucionais que
enquadram a actividade jornalística em Portugal.

Director Maurício Reis

Colaboradores Eduardo Cancela, João Coelho, João Fernandes, João Maia, Marco Santos, Paulo Jorge Dias

Publicidade Cláudio Silva

Marketing Sandra Mendes

Redacção e Publicidade
Rua da Escola, 35 - Coselhas
3020-479 Coimbra
Telef.: 239 081 925
Email geral@informaticafacil.com.pt

Tiragem 10.500 exemplares
Impressão Lidergraf, SA
Rua do Galhano, n.º 15
4480-089 Vila do Conde, Portugal
Distribuição Vasp - Distribuição de Publicações

Publicação Periódica 124077
ISSN 1645-5495
Depósito Legal 374323/14
Proprietário Maurício José da Silva Reis
Contribuinte 175 282 609

#83 » Julho/Agosto/Setembro 2024

LIVRE-SE DAS PASSWORDS ANTIGAS AGORA!

~~12345678~~
~~Pa55word~~
~~W!ndows~~
~~Admin123~~
~~Us3rname~~

Com o roubo de palavras-passe a disparar, nunca foi tão importante livrar-se dos seus logins antigos e inseguros e começar a utilizar substitutos novos e invioláveis - incluindo passkeys. Aqui, explicamos o que deve fazer.

As tentativas de roubo de palavras-passe aumentaram muito nos últimos anos. Em 2015, a equipa de segurança da Microsoft detetou 115 tentativas por segundo. Agora, esse número subiu para mais de 4.000, um aumento de mais de 3.370 por cento. Os piratas informáticos continuam a atacar as palavras-passe porque, no fundo, os seres humanos são previsíveis. Demasiados de nós utilizam as mesmas palavras-passe vezes sem conta, apesar de todos os conselhos de segurança nos dizerem que é uma péssima ideia.

Neste artigo, vamos fazer uma análise completa das palavras-passe, para que possa ver quais as que foram roubadas e o que deve fazer para tornar as suas novas palavras-passe invioláveis. Revelamos uma técnica de criação de palavras-passe que nos tem servido bem ao longo dos anos, e que é mais sofisticada do que substituir a letra 0 por zeros e o número 3 por sinais de euro. Temos a certeza de que tem os seus próprios métodos igualmente engenhosos - por isso, informe-nos.

Também explicamos como se preparar para as passkeys, que estão rapidamente a substituir as palavras-passe. Pode agora utilizá-las em gestores de palavras-passe para iniciar sessão nas suas contas Microsoft, Google e Apple, e em muitos sítios Web. Sabemos que alguns de vós têm dúvidas sobre a segurança e a conveniência das chaves de acesso, mas a indústria tecnológica está a adotar esta tecnologia tão rapidamente que não temos outra opção senão aprender a utilizá-las.

Os nossos conselhos devem ajudá-lo a proteger-se das piores consequências do roubo de palavras-passe, mesmo que as suas contas apareçam em fugas de dados. Por falar nisso, começamos com os nove hacks mais mortíferos dos últimos meses. Se suspeita que foi afetado, tome medidas imediatamente.

A SUA PALAVRA-PASSE FOI DIVULGADA ONLINE?

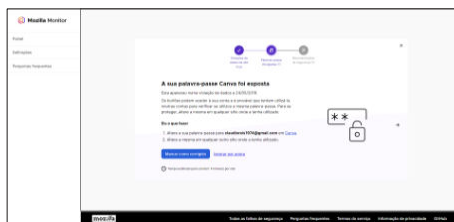
Talvez fique surpreendido com o número de vezes que as suas palavras-passe e nomes de utilizador foram divulgados. Nós ficámos certamente (mais de 300, segundo a Apple)! Adquira o hábito de verificar regularmente se as suas palavras-passe apareceram online utilizando as seguintes ferramentas.

VERIFICAR NA WEB

Como mencionado atrás, o Have I Been Pwned (HIBP, https://tinyurl.com/3hpct98v) é um dos melhores sites para verificar se os seus dados foram roubados. Dirigido pelo especialista em segurança australiano Troy Hunt, é atualizado sempre que surgem notícias de uma violação. Informou-nos que um dos nossos endereços tinha sido violado umas alarmantes 18 vezes. Também permite procurar palavras-passe divulgadas (https://tinyurl.com/5d3ph8ku) - "12345678" aparece quase sete milhões em violações!

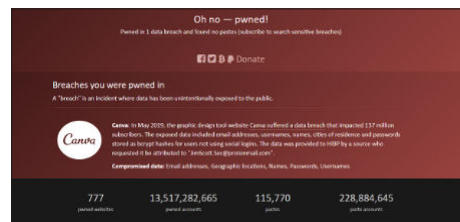
Se não quiser continuar a consultar o HIBP todas as semanas, inscreva-se no serviço "Notify me". Visite https://tinyurl.com/4emf2d4n, escreva o seu e-mail, assinale o Captcha e clique em 'notify me of pwnage'. É-lhe enviado um e-mail que terá de verificar. Depois de o fazer, receberá um e-mail sempre que esse endereço de e-mail aparecer numa nova fuga de dados.

O Mozilla Monitor (https://monitor.mozilla.org), criado pelos criadores do browser Firefox, revelou 30 casos em que o nosso endereço de correio eletrónico e a nossa palavra-passe aparecem online. É compatível com todos os browsers e funciona agora com o gestor de palavras-passe do Firefox para o alertar quando os seus dados são comprometidos. Para o utilizar, é necessário criar uma conta Mozilla em https://tinyurl.com/yrwwjses - clique em Registar no canto superior direito.

Insira o seu endereço de email e depois clique em 'notify me of pwnage'

O Mozilla Monitor disponibiliza links para alterar passwords reveladas, enquanto o HIBP oferece mais informação acerca das brechas de segurança

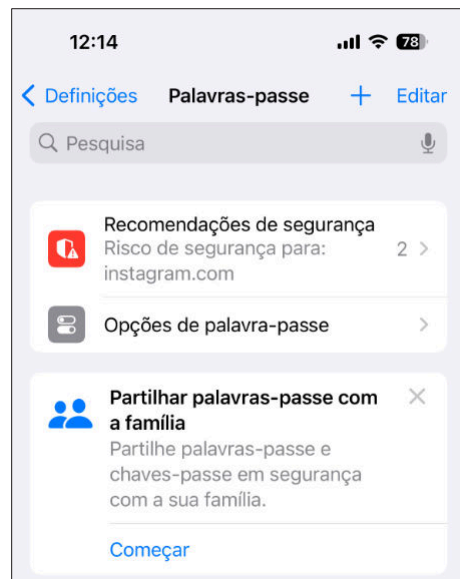
O Mozilla Monitor utiliza a mesma base de dados de violações que o HIBP, pelo que poderá perguntar-se se vale a pena experimentá-lo se já tiver visitado este último. Pensamos que sim porque fornece ligações úteis para alterar as suas palavras-passe nos sítios pirateados.

Por exemplo, o Mozilla diz-nos que a nossa palavra-passe para a rede de fotografia 500px foi exposta e fornece uma ligação para a alterar. Também nos dá a data em que a password foi divulgada. Já o HIBP dá-nos mais informações sobre a violação em si, mas não nos ajuda diretamente a alterar a nossa palavra-passe.

Além disso, ao contrário do HIBP, o Mozilla Monitor disse-nos quando o nosso endereço IP e número de telefone tinham sido divulgados e, uma vez que estes não podem ser alterados, sugeriu medidas que poderíamos tomar para nos mantermos seguros no futuro.

Também deve experimentar o Password Checkup da Google, que está disponível em https://tinyurl.com/h2vc4mvy - anteriormente apenas estava disponível como uma extensão do browser. Continue a ler, para saber mais sobre esta ferramenta.

VERIFIQUE NO SEU TELEMÓVEL OU TABLET

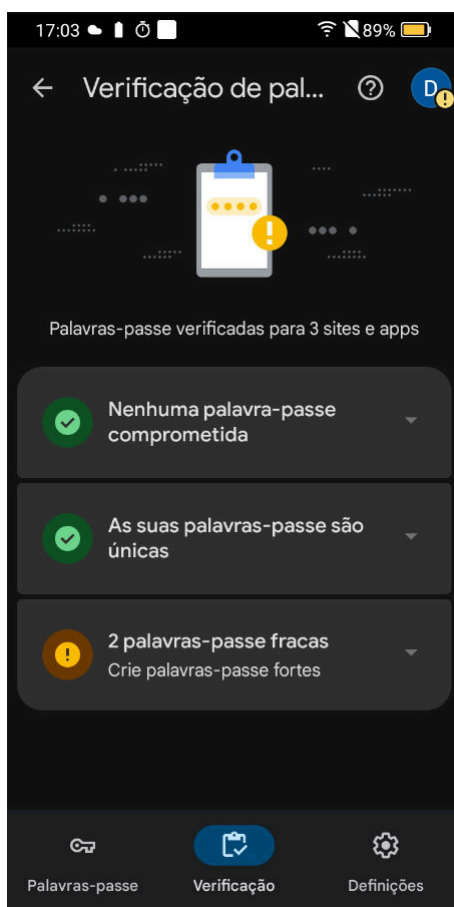
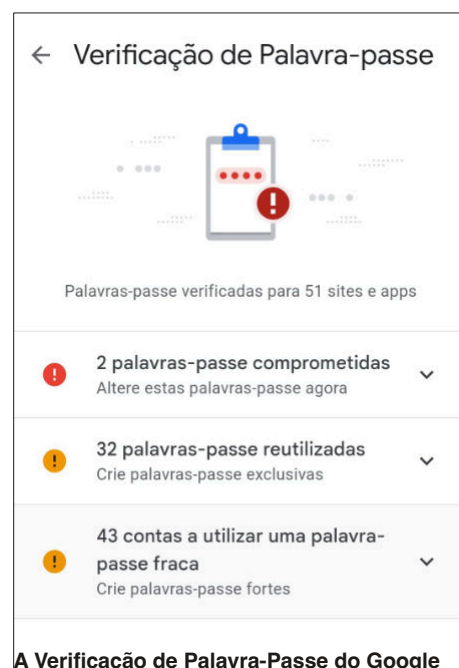
IPHONE E IPAD

No seu dispositivo Apple, abra Definições e, em seguida, toque em Palavras-passe. Na parte superior do ecrã seguinte, verá uma caixa Recomendações de segurança que contém o número de inícios de sessão comprometidos associados às contas que configurou no seu dispositivo ou que guardou no seu Apple keychain.

A Apple avisa-nos que detalhes de pelo menos 2 contas foram revelados

Uma vez que configurámos seis contas no Apple Mail e utilizámos o porta-chaves durante décadas, são apresentadas 322 vulnerabilidades. Tocar na caixa revela quais são, juntamente com uma hiperligação para o site associado a cada uma.

ANDROID

Pode utilizar o Password Checkup da Google no seu telemóvel ou tablet Android, bem como através de um browser (https://tinyurl.com/2y5v7m7j. Abra as Definições e, em seguida, procure por "gestor de palavras-passe" na parte superior. Toque no resultado "Password Manager Google Play services" e, em seguida, na barra de botões Checkup na parte inferior (poderá ser "Check passwords" a azul na parte superior do ecrã, dependendo da sua versão do Android).

O sistema irá agora verificar as palavras-passe que guardou na sua conta Google. Verá as palavras-passe que vazaram, bem como as que foram reutilizadas (todas as nossas são únicas) e as que são suficientemente fracas para serem decifradas por um ataque de força bruta. Toque em "Alterar palavra-passe" para qualquer resultado que pretenda corrigir e será encaminhado para o site relevante ou receberá instruções para abrir a aplicação correspondente, caso a tenha instalada.

A Verificação de Palavra-Passe do Google mostra as passwords comprometidas, as reutilizadas e ainda as que são fracas

Utilizar um gerador de palavras-passe

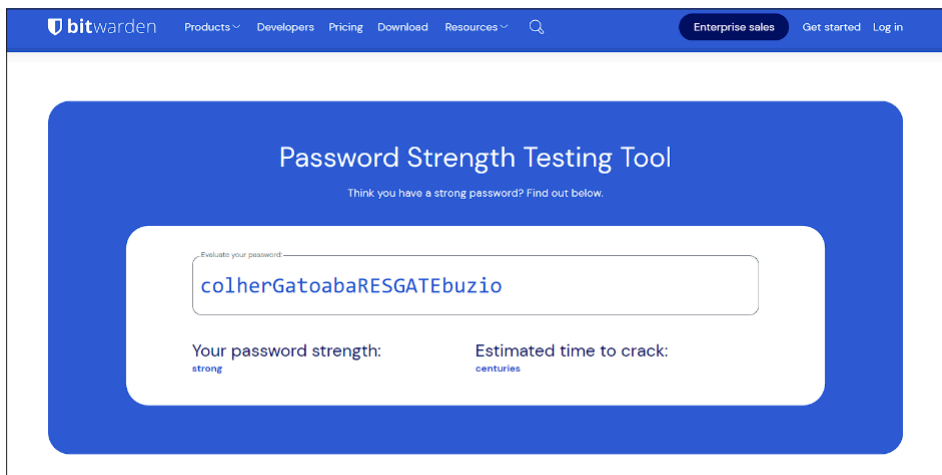
Se tiver dificuldade em criar o seu próprio método de palavra-passe, experimente um gerador de palavras-passe. Os melhores, normalmente provenientes de gestores de palavras-passe, permitem-lhe criar frases-passe (por exemplo, quatro ou cinco palavras aleatórias), bem como palavras-passe e escolher se quer incluir números, letras maiúsculas e caracteres especiais.

A ferramenta da Bitwarden (https://tinyurl.com/bdhsmzrv) faz tudo isto, permitindo-lhe criar palavras-passe com 128 caracteres - embora seja superada pelo www.strongpasswordgenerator.org que permite milhares de caracteres. Também gostamos da ferramenta do LastPass (https://tinyurl.com/y2fyu8m8), especialmente da opção de tornar as palavras-passe "fáceis de ler". Isto evita "caracteres ambíguos" como 1,1,0 e 0.

É claro que os gestores de palavras-passe criam palavras-passe para o encorajar a utilizá-las nas suas ferramentas, mas não tem de o fazer. Basta clicar na opção para a copiar e pode utilizá-la em qualquer lugar.

COMO CRIÁMOS A DERRADEIRA PALAVRA-PASSE IMPOSSÍVEL DE HACKEAR

Uma boa palavra-passe é longa, mas não necessariamente complexa. Não acredita em nós? As estatísticas confirmam-no. A Pivot Point Security explica (https://tinyurl.com/57cssftk) que, com os 94 caracteres de um teclado normal, é possível criar seis quatriliões de palavras-passe únicas de oito caracteres. Encontrar a palavra-passe exata que escolheu levaria oito horas a um computador.

Mas, se escolher uma palavra-passe de 10 caracteres, a mesma máquina demoraria oito dias a decifrá-la - e, se a alargasse para 12 caracteres, ainda estaria a trabalhar nela no ano 2085. Com isto em mente, decidimos criar a

O Bitwarden estima que pode levar séculos (centuries) para piratear a palavra colherGatoabaRESGATEbuzio

derradeira palavra-passe - uma que seja indecifrável mas fácil de memorizar.

TORNE-A POUCO FAMILIAR

Os computadores não entendem palavras, por isso, embora "password" faça muito mais sentido para nós humanos do que "yrhd65tf", um computador vê ambas como uma combinação de oito caracteres aleatórios. É por isso que a complexidade não é necessariamente mais eficaz do que o comprimento.

Em igualdade de circunstâncias, um computador levaria aproximadamente o mesmo tempo a percorrer todas as combinações possíveis até chegar a 'password' do que levaria para 'yrhd65tf, 'zzzzzzzz' ou '12345678'.

No entanto, há um aspeto em que escolher 'password' em vez de 'yrhd65tf' é menos seguro: o facto de aparecer no dicionário. A primeira coisa que um hacker provavelmente fará é submeter o nosso login a um ataque de dicionário, no qual tentará todas as palavras do livro - literalmente - para ver se fomos descuidados. Por isso, vamos evitar palavras reais únicas.

TORNAR A PALAVRA CONFUSA

Como é que podemos combater isto? Temos duas opções: ou inventamos uma sequência aleatória de letras, dígitos e caracteres especiais como #, @ e $, ou combinamos várias palavras do dicionário como colherGatoabaRESGATEbuzio. Podemos até colocar espaços também.

Ao fazê-lo, criámos uma combinação de palavras que é bastante fácil de memorizar, incluindo letras minúsculas e maiúsculas, que é suficientemente longa para demorar "séculos" a decifrar, de acordo com a ferramenta de teste de força da palavra-passe da Bitwarden (https://tinyurl.com/y5ybnxcm).

É claro que essa palavra-passe não satisfaria todos os sítios em que a quiséssemos utilizar porque não tem números nem caracteres especiais, mas agora que temos a nossa frase de base, esses elementos serão fáceis de adicionar e de memorizar.

TORNE-A COMPLEXA

Aumentámos a nossa palavra-passe adicionando 228 ao início, sendo esses dígitos os últimos três do nosso número de telefone, e adicionámos um ponto de exclamação e um símbolo de dólar no meio. A nossa palavra-passe é agora 228colherGatoaba!$RESGATEbuzio. Continua a ser fácil de lembrar, mas é ainda mais complexa do que antes. Se está a pensar porque é que escolhemos um símbolo de dólar, é porque todos os teclados têm $.

TORNE-O ÚNICO

O nosso início de sessão continua a falhar num aspeto muito importante: é uma palavra-passe única, em vez de um sistema. Podemos aprendê-la de cor e usá-la para a Amazon, a BBC, o Facebook e inúmeros outros sites e, durante algum tempo, sentirmo-nos presunçosos e seguros. No entanto, da primeira vez que for pirateada ou divulgada, todas as contas que a utilizam ficarão comprometidas.É por isso que é tão importante utilizar uma palavra-passe diferente para cada início de sessão.

Não é realista esperar que alguém arranje quatro palavras diferentes para cada site, mais números e pontuação, sem as esquecer ou anotar. Por isso, vamos utilizar o mesmo padrão como ponto de partida e, a partir daí, acrescentar algo que o ligue especificamente ao site em que vamos iniciar sessão.

Imaginemos que estamos a criar uma palavra-passe para a Amazon. Pegamos nas duas primeiras letras do seu nome - AM - e adicionamos as palavras do alfabeto fonético para cada uma delas entre os nossos dois caracteres especiais (alphamike). De seguida, fazemos o mesmo para o Facebook (FA, foxtrotalpha), e assim por diante. As nossas palavras-passe seriam todas únicas e indecifráveis.

Pode encontrar o alfabeto fonético em https://tinyurl.com/3rebrhrj, mas se nos sentíssemos muito espertos, poderíamos até criar a nossa própria alternativa ao alfabeto fonético, usando

coisas da nossa casa - desde que nos mantivéssemos consistentes. Se uma destas palavras-passe vazar, só comprometerá o sítio a que se aplica, e não qualquer outro, a menos que também comece com os mesmos dois primeiros caracteres. Mais uma vez, a Bitwarden diz-nos que os três demorariam séculos a decifrar. Boa sorte com isso, piratas informáticos.

CONFIGURAR PASSKEYS PARA MICROSOFT, GOOGLE E APPLE

Desde os anos 60 que utilizamos palavras-passe para proteger os computadores. Isso deu aos piratas informáticos muito tempo para encontrarem formas de as contornar. A autenticação de dois factores (2FA) tem tido algum sucesso no restabelecimento do equilíbrio, tornando a sua palavra-passe efetivamente inútil, a menos que o pirata informático também tenha acesso ao seu telemóvel ou a outro dispositivo físico associado à sua identidade. O passo lógico seguinte é a chave-passe (passkey), que depende completamente desse dispositivo secundário e elimina completamente as palavras-passe.

O processo de configuração de uma nova chave-mestra difere ligeiramente de dispositivo para dispositivo, mas normalmente lê-se um código de barras com o telemóvel e, em seguida, utiliza-se a informação biométrica armazenada nesse dispositivo, como a impressão digital ou uma digitalização do rosto, para confirmar a identidade.

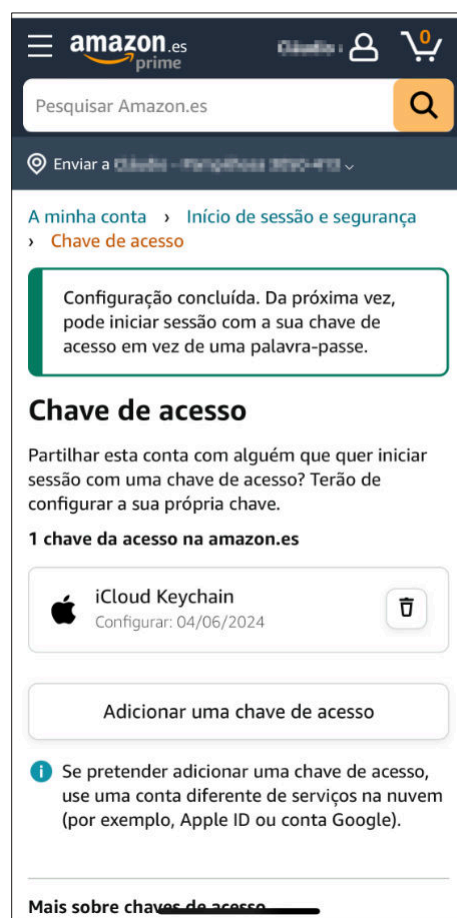
Uma vez feito isso, o telemóvel utiliza a metade da chave de acesso a que tem acesso para desbloquear parcialmente o sítio que visitou. O computador remoto que aloja o sítio faz a mesma coisa com a metade da chave de acesso que retém, e o acesso é-lhe concedido. Para além do facto de as chaves de acesso serem mais simples de utilizar do que as palavras-passe, uma vez que não precisa de se lembrar de nada, consideramos que a vantagem mais evidente é que não pode ser enganado para entrar num site falso. Porquê? Porque um site falso não terá acesso à outra metade da sua chave, como acontece com um site genuíno.

Para demonstrar como funcionam as chaves de acesso, vamos configurar uma chave para a nossa conta Amazon no iOS, Android e Windows, antes de lhe mostrar como proteger as suas contas Microsoft e Google da mesma forma. O processo funcionará de forma semelhante noutros sites que aceitem chaves de acesso.

UTILIZAR CHAVES DE ACESSO (PASSKEYS) NO IPHONE E NO IPAD

As chaves de acesso são suportadas no iOS 16 e no iPadOS 16 (lançado em 2022) ou posterior em dispositivos com autenticação de dois factores e que tenham as Chaves de iCloud ativadas. Estas chaves são suportadas há muitos anos, pelo que é muito provável que já estejam disponíveis no seu dispositivo, mas vale a pena verificar antes de avançar.

Abra as Definições e toque no seu nome na parte superior do ecrã. Toque em "Iniciar sessão e segurança" e verifique se a autenticação de dois factores está ativada a meio do ecrã. Se não estiver, toque em "Ativar autenticação de dois factores" seguido de Continuar. Introduza um número de telefone que controle e toque em Seguinte, e a Apple enviará um código para esse número. Introduza este código no seu telemóvel ou tablet para concluir o processo de configuração da autenticação de dois factores.

Para verificar se as Chaves de iCloud estão activadas, volte ao ecrã inicial das

Entrámos no nosso iPhone com a nossa face para guardar a passkey da Amazon

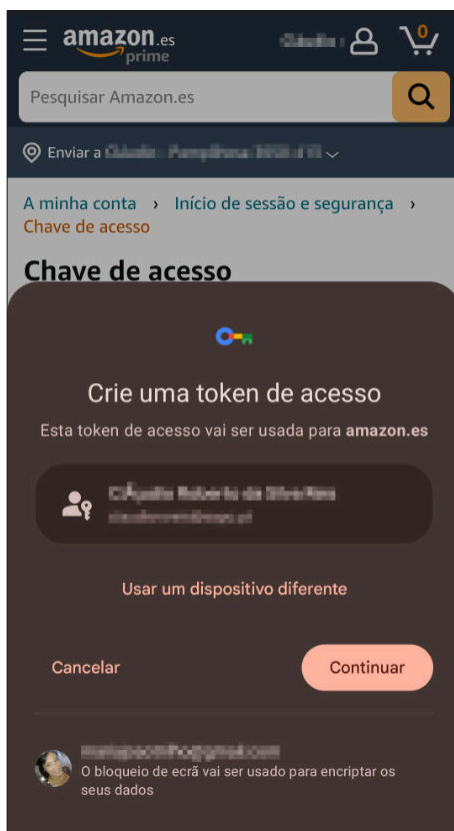
Definições e toque novamente no seu nome na parte superior do ecrã. Toque em ID iCloud (ID Apple) seguido de 'Palavras-passe e porta-chaves". Se o porta-chaves não estiver ativado, ative-o e siga as instruções no ecrã para concluir o processo.

Agora, visite www.amazon.es (por exemplo) no browser do seu telemóvel ou tablet. Inicie sessão na sua conta da forma habitual e, em seguida, toque no seu nome na parte superior do ecrã. Toque no botão 'Ver todos' ao lado de 'A minha conta' no menu da barra lateral que aparece, seguido de 'Início de sessão e segurança' na secção Configurações da conta.

Desloque-se para baixo até à secção Chave de acesso e toque em "Configurar", seguido do botão amarelo "Configurar" no ecrã seguinte. Aparece agora a caixa de desbloqueio normal a pedir-lhe que utilize o método biométrico que configurou no seu dispositivo para criar a chave de acesso. No nosso iPhone, iniciamos sessão utilizando o Face ID, por isso, nesta altura, é-nos perguntado se queremos utilizar o Face ID para iniciar sessão. Se o fizermos, tocamos em Continuar e o ecrã digitaliza o nosso rosto. Depois de nos reconhecer, cria a chave-mestra.

UTILIZAR CHAVES DE ACESSO EM DISPOSITIVOS ANDROID

As chaves de acesso são suportadas em dispositivos com Android 9 (lançado em 2018) e posterior. Visite www.amazon.es no seu dispositivo Android e, em seguida, inicie sessão. Toque no seu nome na parte superior do ecrã, seguido do botão 'Ver todos' ao lado de 'A minha conta' e, em seguida, em 'Início de sessão e segurança'. Desloque-se para baixo até à Chave de acesso e toque em 'Configurar', seguido de 'Configurar' (ou "Adicionar uma chave de acesso" se já tiver criado uma chave de acesso utilizando um dispositivo diferente).

O Android mostra-lhe o início de sessão da Amazon para o qual está a configurar uma chave de acesso e a conta Google que será utilizada para armazenar a chave de acesso e

Verá a conta da Amazon para a qual está a criar a passkey e a conta Google onde vai ser guardada

sincronizá-la entre os seus dispositivos. Se pretender alterar a conta Google associada, toque na mesma e selecione uma alternativa no menu.

Uma vez configurada, a sua chave-mestra será desbloqueada utilizando o processo que utiliza para desbloquear o telemóvel. Toque em 'Utilizar bloqueio de ecrã' e ser-lhe-á pedido que desbloqueie o dispositivo. No nosso caso, foi-nos pedido que tocássemos no sensor de impressões digitais na parte de trás do nosso telemóvel Pixel 5. Depois de o fazermos, o processo foi concluído e a chave-mestra foi adicionada à nossa conta Amazon.

UTILIZAR CHAVES DE ACESSO EM PCS COM WINDOWS

Também pode utilizar o Windows para guardar as suas chaves de acesso, desde que esteja a utilizar pelo menos o Windows 11 com a atualização Moment 4. Depois de guardar uma chave-mestra no sistema operativo, esta pode ser desbloqueada utilizando qualquer processo que utilize para iniciar sessão no Windows (PIN, reconhecimento facial, etc.).

Para proteger uma conta Amazon, inicie sessão em www.amazon.es utilizando o seu browser normal, passe o rato sobre "Account & Lists" na barra na parte superior do ecrã e clique em Your Account no menu que aparece. Clique em "Login & Security" (Iniciar sessão e segurança) e, em seguida, inicie novamente sessão para aceder às definições pretendidas. Toque em "Configurar" ao lado de Chave de acesso e, no ecrã seguinte, clique em 'Adicionar uma chave de acesso'.

Aparecerá uma janela de Segurança do Windows a pedir-lhe que inicie sessão utilizando as mesmas credenciais que utiliza para iniciar sessão no Windows.

Depois de clicar em 'Adicionar uma chave de acesso' o Windows vai pedir para fazer login com as mesmas credenciais que usa para iniciar sessão no Windows

Que sítios Web suportam as chaves de acesso?

As chaves de acesso estão a crescer rapidamente - só a Google afirma que já protegem mais de 400 milhões de contas. A razão é que muitos sítios Web permitem agora iniciar sessão com elas. Estes incluem a Amazon (como já explicámos), bem como o Dropbox, eBay, Nvidia, PayPal e WhatsApp. A lista mais completa que vimos online está no site da FIDO Alliance https://tinyurl.com/5fhfucv3, que atualmente lista 131 serviços. É atualizada regularmente, por isso não deixe de a consultar.

Assim que o fizer, será criada e guardada uma chave de acesso no Windows, que pode agora utilizar para iniciar sessão na Amazon.

CONFIGURAR CHAVES DE ACESSO PARA CONTAS MICROSOFT E GOOGLE

Agora que já configurou chaves de acesso para a sua conta Amazon, deve fazer o mesmo para outras contas em sites que suportem o processo. Recomendamos que comece pelas suas contas Microsoft e Google.

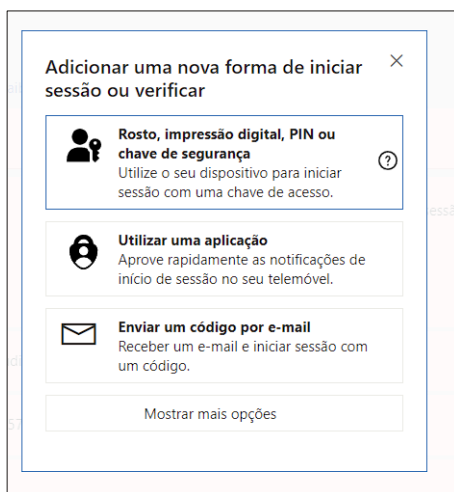
CONTA MICROSOFT

Depois de adicionar as chaves de acesso ao Windows 11 no ano passado, a Microsoft permite-lhe agora iniciar sessão em todas as suas contas de "consumidor". Isto significa que pode iniciar sessão no Office, OneDrive, Outlook,

Skype, Windows e Xbox utilizando o seu rosto ou impressão digital.

Visite https://tinyurl.com/2mntyra5 e inicie sessão utilizando o seu nome de utilizador e palavra-passe Microsoft existentes. Na parte inferior, clique na ligação azul "Adicionar uma nova forma de iniciar sessão ou verificar". Aparecerá uma janela de Segurança do Windows.

Clique em "Rosto, impressão digital, PIN ou chave de segurança" nesta nova janela e o site perguntará onde pretende guardar a sua chave de acesso.

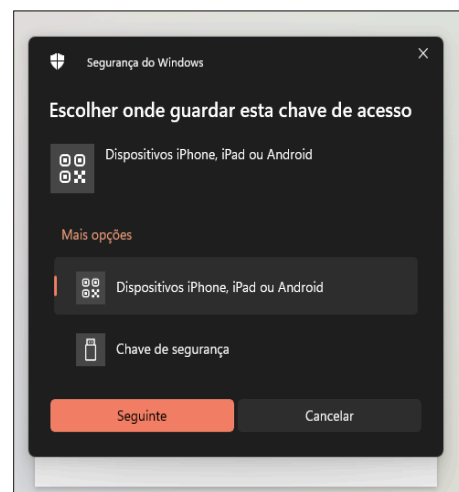
A opção predefinida é "iPhone, iPad ou dispositivo Android". Partindo do princípio de que pretende utilizar o seu dispositivo móvel, deixe esta opção selecionada e clique em Next (Seguinte). As opções serão substituídas por um código QR. Deixe-o no ecrã e abra a aplicação da câmara no seu

Clique em 'Rosto, impressão digital, PIN ou chave de segurança' e depois selecione onde quer gravar a sua chave de acesso (passkey)

telemóvel ou tablet. Aponte a câmara para o código QR e aparecerá no ecrã do seu telemóvel uma opção para "Guardar uma chave de acesso". Toque nesta opção.

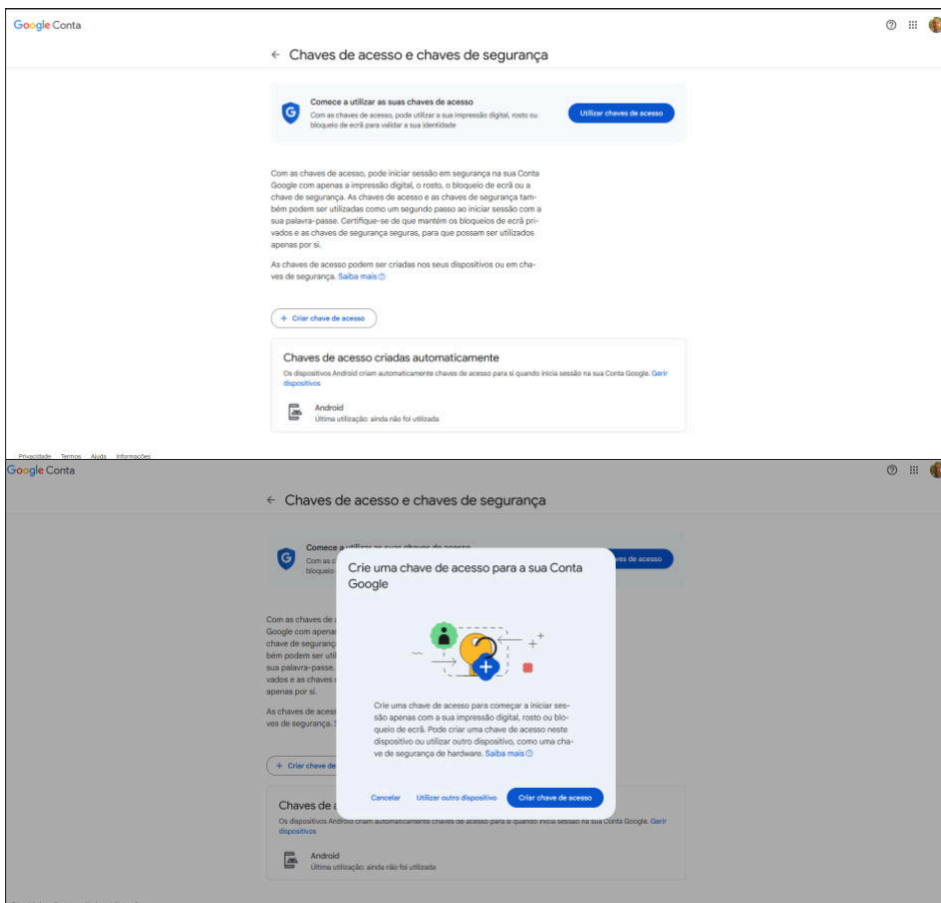
Será apresentada uma janela "Iniciar sessão" no seu dispositivo, pedindo-lhe que utilize o seu início de sessão biométrico para confirmar a sua identidade. Toque em "Continuar" e, em seguida, utilize o ID Facial ou a impressão digital para desbloquear o dispositivo. Depois de ter sido reconhecido, verá a janela Segurança do Windows no seu PC mudar para confirmar que "Pode agora utilizar o seu dispositivo para iniciar sessão em 'login.microsoft. com'".

Clique em Seguinte e, em seguida, dê um nome à sua chave-mestra. Como configurámos a nossa chave de acesso num iPhone, que a guardou no iCloud Keychain, a partir do qual pode ser sincronizada entre dispositivos, o processo sugere o Apple iCloud Keychain. Vamos manter esta opção, clicando em Seguinte.

CONTA GOOGLE

A Google está a promover as chaves de acesso em grande escala e está a trabalhar com empresas como a Adobe, eBay, Nintendo, PayPal e Uber para garantir a sua adoção. Lançou também a sua primeira Titan Security Key capaz de armazenar chaves de acesso. Tem capacidade para 250 e está disponível nas versões USB-A e USB-C, cada uma com um preço de 30 libras na loja da Google: https://tinyurl.com/mss4rdee.

Visite https://tinyurl.com/33aep9jz e inicie sessão na conta Google para a qual pretende criar uma chave de acesso. Agora, clique em "Criar uma chave-mestra" - nessa altura, uma janela do Windows Security pedir-lhe-á para iniciar sessão. Escolha o seu método preferido.

Assim que tiver iniciado sessão, o Windows guarda a chave-mestra, tal como fez anteriormente para a conta Amazon. Para verificar se é possível utilizá-la para iniciar sessão, abra uma nova janela privada do navegador (prima Ctrl+Shift+N num navegador baseado no Chrome), visite www.google.pt e clique em Iniciar sessão.

Agora, introduza o endereço de correio eletrónico associado à conta para a qual

Inicie sessão na sua conta Google para a qual quer configurar uma chave de acesso, depois clique em 'Utilizar chaves de acesso' e depois no botão 'Criar chave de acesso'

acabou de criar uma chave de acesso e clique em Seguinte. Quando lhe for pedido para "Introduzir a sua palavra-passe", clique em "Tentar de outra forma" seguido de "Utilizar a sua palavra-passe". A janela Segurança do Windows voltará a aparecer, pedindo-lhe que utilize a sua opção de início de sessão normal do Windows (o PIN, no nosso caso) para desbloquear a sua conta Google. Faça o que lhe é pedido e clique em Seguinte para concluir o processo.

Quando utiliza um gestor de palavras-passe, já não precisa de se lembrar de nenhuma palavra-passe. Este pode gerar um início de sessão único para cada sítio e guardá-lo num cofre online, permitindo-lhe utilizá-lo em todos os seus dispositivos.

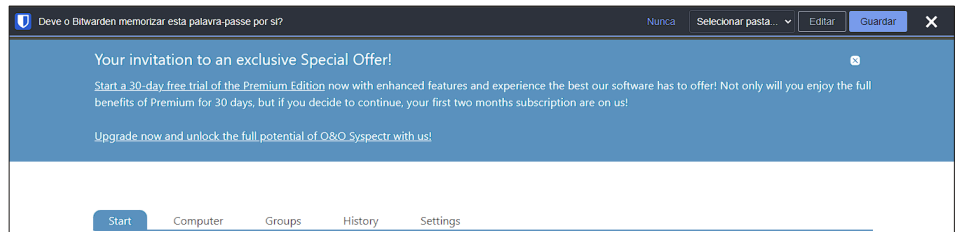
O nosso gestor de palavras-passe favorito é o Bitwarden, disponível como aplicação para iOS (https://tinyurl.com/tfewdkx7) e Android (https://tinyurl.com/2nk7a2xk), bem como um programa para Windows e uma extensão para o browser (https://tinyurl.com/2p86rn7n).

Recomendamos, no mínimo, a instalação da extensão para o seu navegador, mesmo que não descarregue o software, uma vez que pode utilizá-la para guardar palavras-passe no seu cofre Bitwarden e introduzi-las automaticamente quando visita um site.

Uma das razões pelas quais gostamos particularmente do Bitwarden, para além do facto de o plano gratuito oferecer tudo o que é provável que precise, é o de ser frequentemente atualizado. No ano passado, adicionou suporte para chaves de acesso, pelo que pode ser utilizado como o iCloud Keychain, o Password Manager da Google ou o Windows, para armazenar e sincronizar as suas chaves de acesso.

Esta é uma boa notícia se trabalhar com vários dispositivos, porque poderá configurar uma única chave de acesso que será partilhada por todos eles, em vez de ter uma chave de acesso diferente para cada sistema operativo.

CONFIGURAR O BITWARDEN

Aceda a www.bitwarden.com, clique em 'Get started' (Começar) na parte superior e, em seguida, introduza o seu endereço de e-mail e nome, bem como uma palavra-passe mestra. Esta é a única palavra-passe que terá de

Clique em 'Guardar' para armazenar as suas credenciais de acesso no seu cofre do Bitwarden

memorizar a partir deste ponto - é vital que não se esqueça dela (siga os nossos conselhos para criar um início de sessão indecifrável mas fácil de memorizar). O processo de configuração também lhe pede uma dica de palavra-passe. Mais uma vez, faça com que seja um pouco enigmática, para que se possa lembrar dela, mas sem revelar o jogo.

Agora, instale a extensão para o seu navegador e clique no ícone do quebra-cabeças (ou cubo no Opera) seguido do pino junto ao nome do Bitwarden. Isto irá fixar o ícone do escudo do Bitwarden na barra do seu navegador. Na próxima vez que entrar num site, o Bitwarden deve detetar que digitou um nome de utilizador e uma palavra-passe e oferecer-se para os guardar.

Clique em Guardar para memorizar os seus dados.

Da próxima vez que precisar de iniciar sessão no mesmo site, em vez de escrever os seus dados manualmente, clique com o botão direito do rato no campo do nome de utilizador ou da palavra-passe e passe o cursor sobre Bitwarden. Em seguida, passe o cursor sobre 'Auto-fill login' e clique em 'Log in to your vault'. Introduza a sua palavra-passe mestra na janela que aparece e o Bitwarden preencherá o seu nome de utilizador e palavra-passe.

GUARDAR CHAVES DE ACESSO NO BITWARDEN

Para guardar uma chave de acesso no seu cofre Bitwarden, siga o mesmo procedimento que seguiria para guardar uma chave no Windows. Para a Amazon, por exemplo, navegue até as configurações da sua conta como anteriormente, clique em 'Login & Security' e, em seguida, clique no botão Edit ao lado de Passkey.

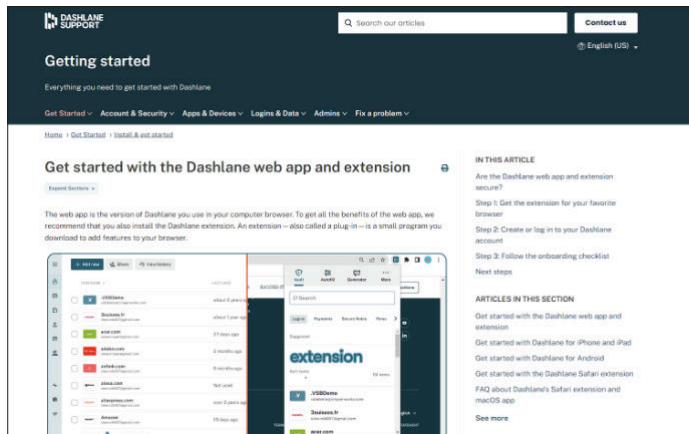
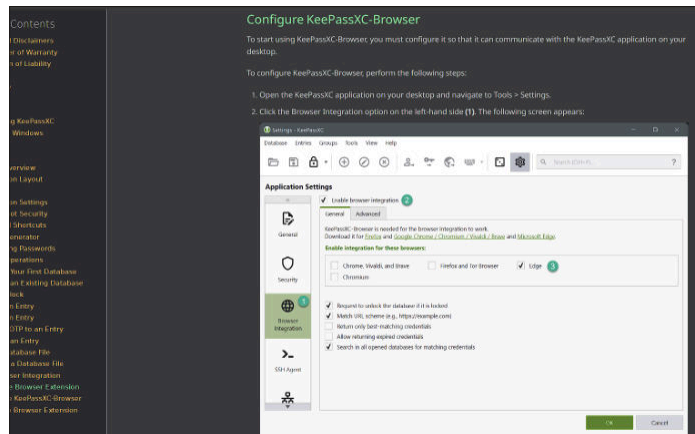
No ecrã seguinte, clique em 'Add a passkey' e, desta vez, em vez de aparecer uma janela de Segurança do Windows, será aberta a janela pop-up do Bitwarden. Digite sua senha do Bitwarden para desbloquear sua conta e clique em 'Save passkey as new login' (Salvar senha como novo login) para armazená-la no seu cofre. Da próxima vez que pretender iniciar sessão na sua conta Amazon, quando lhe for pedida a sua palavra-passe, clique no botão "Iniciar sessão com uma chave de acesso". Quando o fizer, a janela Bitwarden voltará a aparecer e, tendo detectado o sítio a que está a tentar aceder, sugerirá a chave de acesso mais adequada do seu cofre. Clique em Confirmar e iniciará sessão.

OUTROS GESTORES DE SENHAS COM PASSKEYS

O Bitwarden está longe de ser o único gestor de palavras-passe a adicionar suporte para chaves-chave. O 1Password introduziu-as em setembro passado para iOS e Windows, e alargou-as ao Android (versão 14) em março - ver https://tinyurl.com/5m7kexjk.

O Dashlane implementou uma versão das chaves de acesso em dezembro, embora utilize o seu próprio sistema de segurança "sem palavra-passe" e não a tecnologia FIDO, que foi desenvolvida pela Apple, Google e Microsoft e que se tornará provavelmente a norma universal - ver https://tinyurl.com/2zj2296r.

Entretanto, o KeePassXC adicionou as chaves de acesso em março, embora seja necessário instalar a sua extensão do browser para as utilizar - encontre as ligações relevantes em https://tinyurl.com/y9az467f. Também é necessário selecionar Ativar chaves de acesso nas definições da extensão. Consulte https://tinyurl.com/ystp3k75 para obter mais instruções.

Ainda não há sinais de que o LastPass suporte as chaves de acesso, apesar de ter dito, há um ano, que o suporte estaria para breve (https://tinyurl.com/mr2b8pwn). Mas com a empresa a sofrer duas violações graves em 2022, que afectaram 30 milhões de utilizadores, aconselhamos que se mantenha afastado de qualquer forma. ■

O KeePassXC e o Dashlane são outras duas boas opções para gerir as suas palavras-passe e chaves de acesso

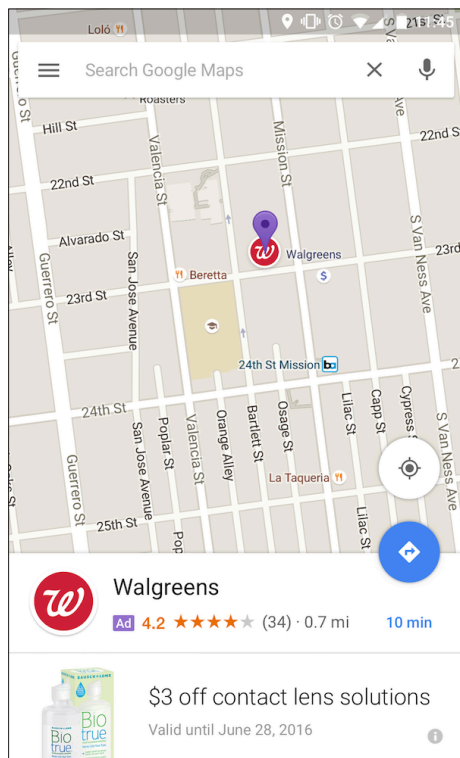
DEIXE DE USAR O GOOGLE MAPS

O Google Maps é a aplicação mais popular para explorar o mundo, mas nos últimos tempos tem vindo a decair. Neste artigo, explicamos o que correu mal e o que deve utilizar em vez dela.

PORQUE DEVE ABANDONAR O GOOGLE MAPS

OS SEUS MAPAS ESTÃO CHEIOS DE PINS E ANÚNCIOS

Uma das melhores coisas do Google Maps é a possibilidade de fazer zoom para ver os nomes das lojas, restaurantes e outras comodidades, para que saiba o que está disponível numa zona antes de lá chegar. No entanto, nos últimos anos, os mapas do Google Maps tornaram-se demasiado confusos com pins e marcadores coloridos.

Por exemplo, existem pins cor-de-rosa para hotéis, cor de laranja para bares e restaurantes, marcadores azuis claros para locais culturais e azuis escuros para lojas. Alguns pins também têm fotografias ou logótipos, ou são quadrados com um ponto no meio, o que indica que são anúncios de empresas que pagaram para serem incluídas no mapa.

Os pinos promocionais para negócios são agora inevitáveis no Google Maps

Individualmente, estes marcadores e pins promocionais são fáceis de ignorar, mas a quantidade agora apresentada pelo Google Maps torna-os perturbadores, especialmente quando ocultam detalhes do mapa que está a tentar ver.

Além disso, ao contrário dos anúncios na Pesquisa Google, estes pins são muitas vezes irrelevantes para o que está a procurar e tem de reduzir o zoom do mapa para os ocultar.

O NOVO ESQUEMA DE CORES É MAIS DIFÍCIL DE LER

Em novembro passado, o Google Maps introduziu um novo esquema de cores mais suave que desagradou a muitos utilizadores. As estradas são agora cinzentas em vez de brancas ou amarelas, enquanto os parques e a água têm tons mais claros de verde e azul.

Descrito como "mais frio, menos exato e menos humano" por um antigo designer do Google Maps (https://tinyurl.com/yckx7m48), existem também preocupações de que os mapas redesenhados sejam mais difíceis de ler para as pessoas daltónicas. Mudar para o modo escuro da aplicação torna as características do mapa mais fáceis de distinguir, mas questionamos por que razão a Google teve de alterar o esquema de cores predefinido com que todos estavam satisfeitos.

ESTÁ SEMPRE A ADICIONAR FUNCIONALIDADES SOCIAIS SEM SENTIDO

Estaríamos (literalmente) perdidos sem as ferramentas essenciais do Google Maps, como as direções, o Street View e os mapas offline, mas a sua aplicação móvel está a transformar-se cada vez mais numa rede social. Embora possa ser útil ler as opiniões de outros utilizadores sobre restaurantes, hotéis e lojas, será que precisamos mesmo de ver fotografias e vídeos das suas comidas, bebidas e compras, especialmente numa posição tão proeminente no separador Explorar?

O Google Maps foca-se agora mais nas características sociais do que em ferramentas de navegação

Pode até "seguir" guias e colaboradores locais, para receber atualizações sobre as suas últimas descobertas - uma funcionalidade copiada e mais adequada ao Instagram e ao TikTok.

As recentes adições à aplicação Mapas

incluem "listas colaborativas", que permitem convidar amigos e familiares para avaliarem os locais que sugerir utilizando emojis; uma nova ferramenta de IA que fornece "inspiração visual" para atividades a realizar; e - recentemente lançada nas principais cidades dos EUA - uma lista semanal de "tendências" dos mais recentes "pontos quentes". Nada disto o vai levar de A a B mais depressa.

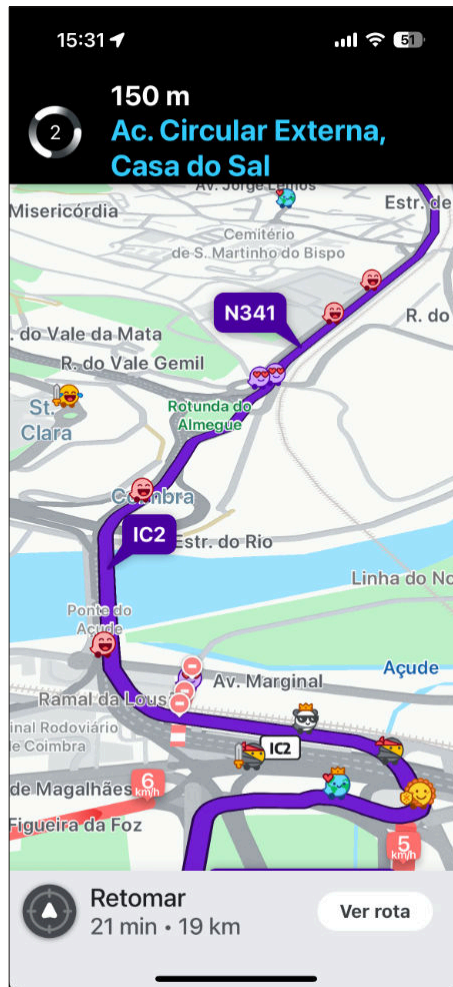
NEM SEMPRE MOSTRA OS NOMES DAS RUAS

Com tantos elementos a ocuparem o seu layout, o Google Maps esquece-se frequentemente de mostrar as informações mais importantes - como o nome da rua que está a visualizar. Faça zoom para a sua localização atual ou para um local que não tenha procurado especificamente e, mais frequentemente, o Google Maps não lhe diz o nome da estrada.

Isto acontece mesmo nas estradas principais, embora a aplicação possa apresentar o número da estrada A, o que não ajuda muito os peões que procuram sinais de trânsito. Tocar numa estrada adjacente normalmente faz com que o Google Maps identifique a estrada atual, mas não deixa de ser uma omissão frustrante.

UTILIZE ESTAS APLICAÇÕES DE NAVEGAÇÃO

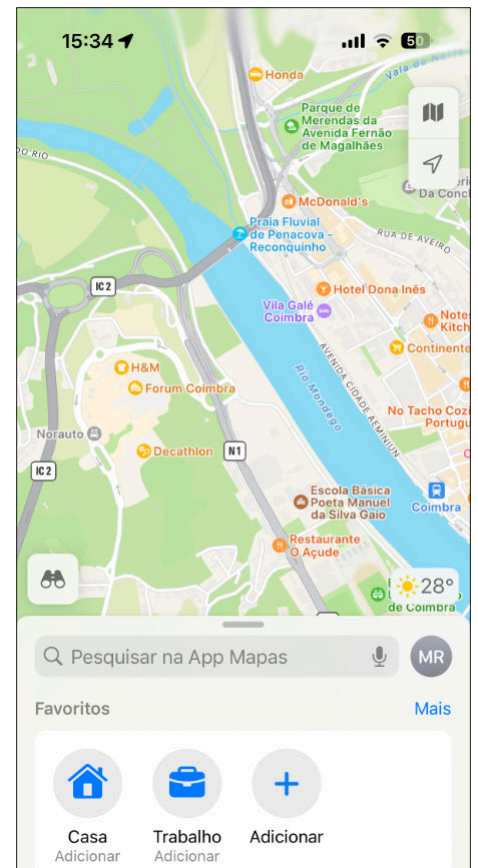
MELHOR PARA CONDUZIR
Waze
www.waze.com

Embora o Waze também seja propriedade da Google, é uma

O Waze oferece bastantes informações de trânsito em tempo real incluindo alterações da velocidade limite

aplicação de navegação melhor para os condutores, fornecendo direções passo a passo e informações de trânsito em tempo real sem distrações. Em vez de se limitar a indicar-lhe o caminho mais rápido para o seu destino e deixá-lo entregue a si próprio, o Waze analisa constantemente as condições de condução para o ajudar a evitar engarrafamentos, obras na estrada e acidentes, bem como outros perigos, como lombas, buracos e até mau tempo.

Ao contrário do Google Maps, o modo mãos-livres da aplicação oferece uma escolha de vozes (incluindo as de celebridades e a sua própria), enquanto a comunidade Waze fornece dados verdadeiramente úteis em tempo real a outros utilizadores - e não fotografias do local onde almoçaram na semana passada. Gostamos particularmente da nova opção que fornece alertas visuais e de voz quando um limite de velocidade está prestes a diminuir ao longo do seu percurso, para que tenha tempo de abrandar.

MELHOR PARA A PRIVACIDADE
Mapas da Apple
https://tinyurl.com/mr3p5pmu

O Mapas está instalado em todos os iPhones e iPads, mas pode continuar a utilizar o Google Maps por defeito. É uma pena, porque a aplicação da Apple melhorou consideravelmente nos últimos anos e a sua abordagem

O Mapas da Apple tem uma interface mais limpa do que o Google Maps, sem distrações

"menos é mais" torna-a mais agradável aos olhos.

A barra de pesquisa permite aceder facilmente ao histórico de pesquisas, às localizações guardadas e às informações sobre empresas e locais, sem obstruir a vista, e os mapas são detalhados mas organizados. Além disso, o Mapas oferece a maior parte das mesmas funcionalidades que o Google Maps, incluindo direcções, horários de transportes públicos e controlo mãos-livres (utilizando o Siri), embora o seu equivalente no Street View - Look Around - não seja tão abrangente.

Ao contrário do Google, a Apple respeita a privacidade do utilizador. Oculta a sua localização real quando planeia percursos e não recolhe dados sobre as suas pesquisas no Google Maps para lhe apresentar anúncios e recomendações.

MELHOR PARA MAPAS OFFLINE

MapFactor Navigator
https://tinyurl.com/3vmp8p3e

Muitas aplicações de navegação oferecem mapas offline, mas esta aplicação é especializada neles, permitindo-lhe encontrar o seu caminho quando perde a ligação à Internet. Vá ao "Gestor de mapas", na secção Ferramentas, para descarregar mapas de países inteiros ou apenas de regiões específicas, que são obtidos e mantidos atualizados pela comunidade OpenStreetMap. Pode então procurar o seu destino e as paragens pretendidas e especificar o seu meio de transporte (por exemplo, carro, bicicleta, autocarro, autocaravana ou a pé), para planear o seu percurso e obter indicações passo a passo, mesmo quando não tem sinal de telemóvel. Algumas funcionalidades, como as atualizações de trânsito em tempo real e os mapas de navegação por satélite TomTom, requerem uma subscrição Navigator Pro ou suplementos pagos.

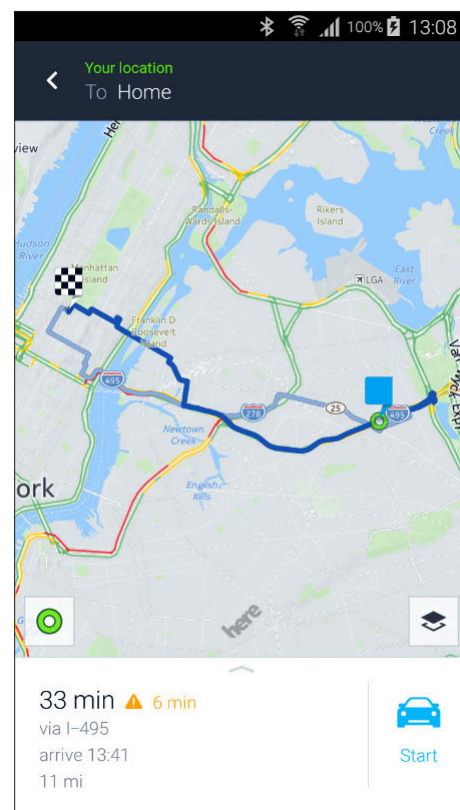
O MELHOR EM TERMOS DE FUNCIONALIDADES

Here WeGo
https://tinyurl.com/3k76nvwt

O Here WeGo também tem mapas offline, bem como muitas outras funcionalidades úteis que fazem dele o rival gratuito mais próximo do Google Maps e do Apple Mapas.

Fornece direções porta-a-porta para conduzir, andar de bicicleta, a pé e de transportes públicos, em formato escrito, falado e em mapa; actualizações de trânsito em tempo real, incluindo detalhes sobre limites de velocidade e câmaras; um "modo noturno" que protege os seus olhos quando viaja à noite; e a opção de guardar o local onde estaciona.

Tal como no Google Maps, pode aplicar diferentes camadas à vista do mapa, como Satélite (ver imagem do ecrã à esquerda), Terreno e 3D, e fazer zoom para ver lojas, restaurantes, atracções turísticas e muito mais, sem se distrair com anúncios e recomendações.

O Here WeGo até mostra a meteorologia da zona no canto superior esquerdo - uma funcionalidade que a Google só recentemente adicionou - e é compatível com o Android Auto e o Apple CarPlay. ■

O Here WeGo permite-lhe aplicar diferentes camadas aos seus mapas incluindo satélite

Mude para uma versão mais leve do Google Maps

Se gosta da aplicação principal do Google, o Maps, mas não gosta das alterações recentemente introduzidas, considere instalar o Google Maps Go (https://tinyurl.com/bdy79zf5) no seu telemóvel Android.

Esta versão simplificada concentra-se em fornecer direções (de carro, de bicicleta ou a pé) e em destacar locais de interesse, sem qualquer dos disparates sociais que agora prejudicam o fornecimento de informações sobre empresas e avaliações de clientes.

Embora não seja possível descarregar mapas para ver offline, o Google Maps Go inclui outras funcionalidades úteis, como os horários dos transportes públicos, actualizações de trânsito e camadas de mapas. É muito mais rápido a carregar e mais fácil de navegar do que a aplicação completa do Google Maps, obtendo informações através do Chrome em vez de acumular uma grande quantidade de dados.

Acelere o seu computador portátil sem gastar um cêntimo

Todos desejamos que nosso computador funcione de maneira plena, rápida e estável, mas isso nem sempre ocorre, especialmente com portáteis. Neste artigo, oferecemos algumas sugestões gratuitas que pode experimentar para melhorar o desempenho do seu PC.

Todos nós temos expetativas em relação aos nossos computadores portáteis. Queremos que funcionem de forma rápida e nos permitam passar o que quer que seja que estamos a tentar fazer, seja um grande projeto de trabalho ou o próximo nível do nosso jogo de vídeo favorito. Infelizmente, há muitas ocasiões em que os nossos computadores portáteis nos desiludem, funcionando lentamente e fazendo com que toda a produtividade seja interrompida. Recuperar esse desempenho não tem de ser difícil e existem algumas coisas que pode tentar fazer para aumentar a velocidade de forma gratuita.

A maioria dos portáteis atuais possuem ferramentas que permitem tirar máximo partido do sistema

Se está a tentar fazer com que o seu computador portátil funcione mais fluidamente e se pareça um pouco mais com o dia em que o comprou (ou se acabou de comprar um e acha que não está a funcionar tão depressa como poderia), aqui estão algumas coisas gratuitas que pode experimentar para o melhorar.

1. GARANTIR QUE ESTÁ A UTILIZAR O PERFIL DE POTÊNCIA IDEAL

Este é um ponto importante. Se selecionar o perfil de energia errado, pode perder imenso desempenho. Se o computador portátil pensar que quer que ele funcione silenciosamente ou a frio, pode não permitir que a CPU e a GPU atinjam todo o seu potencial.

Em muitos computadores portáteis, é comum encontrar planos de energia do Windows, bem como planos especiais do fabricante. Quase todos os portáteis para jogos que encontrar terão um software de gestão do sistema pré-instalado que inclui toda a gestão do perfil de energia de que pode necessitar, e o mesmo está a tornar-se cada vez mais comum nos portáteis de uso geral, mas, a menos que saiba procurá-lo, terá de o deixar na configuração em que o portátil foi enviado.

Numa máquina com Windows 11, abra 'Definições', selecione 'Sistema' e, em seguida, 'Energia e bateria'. Nesta página, procure o 'Modo de energia' e defina-o para 'Melhor desempenho'.

Em seguida, procure quaisquer ferramentas pré-instaladas pelo fabricante do seu computador portátil. Alguns exemplos são o Lenovo Legion Arena, o Alienware Command Center, o Razer Synapse e o Acer Predator Sense. Nestas ferramentas, deve ser possível encontrar diferentes perfis de energia (certifique-se de que o computador está ligado à corrente para ver todas as opções) que lhe permitirão levar o sistema ao seu potencial máximo.

Se quiser ir ainda mais longe, pode experimentar o undervolting.

2. DESCARREGUE OS DRIVERS DE GPU MAIS RECENTES

Quer tenha um computador portátil para jogos ou uma estação de trabalho, se o seu sistema tiver uma GPU discreta e esta não estiver a funcionar com os controladores mais recentes, pode estar a perder muito desempenho.

Os controladores ajudam a otimizar o manuseamento de aplicações selecionadas pelas GPUs e podem fazer uma grande diferença. Nos últimos anos, os gráficos Arc da Intel têm sido um exemplo perfeito disto, registando enormes aumentos de desempenho com as atualizações dos controladores.

A AMD, a Nvidia e a Intel dispõem de ferramentas diferentes para atualizar os respectivos controladores, pelo que deve pesquisar os componentes do seu computador para encontrar o método de atualização adequado.

3. AJUSTAR AS "OPÇÕES DE DESEMPENHO" DO WINDOWS

O seu computador portátil funciona com o Windows, mas também o Windows funciona no seu computador portátil, o que significa que tem as suas próprias despesas gerais. Consome recursos, ocupa ciclos de relógio e faz

O que é o undervolting?

O undervolting é uma técnica usada para reduzir a voltagem fornecida a um componente eletrónico, como um processador ou uma placa gráfica, com o objetivo de diminuir o consumo de energia e o calor gerado, sem comprometer significativamente o desempenho. Geralmente, isso é feito ajustando as configurações no BIOS ou por meio de software especializado. Ao reduzir a voltagem, os componentes consomem menos energia e produzem menos calor, o que pode ajudar a prolongar sua vida útil e reduzir o ruído do sistema. No entanto, é importante realizar o undervolting com cuidado, pois ajustes excessivos podem levar a instabilidade ou mau funcionamento do sistema.

O processo de undervolting pode variar dependendo do componente que deseja ajustar, mas aqui está um guia geral passo a passo:

1. Pesquisa e preparação: Antes de começar, pesquise sobre o seu componente específico (processador, placa gráfica, etc.) para entender os seus limites de voltagem e as ferramentas disponíveis para realizar o undervolting. Certifique-se de ter um software confiável para realizar os ajustes.

2. Software de undervolting: Descarregue e instale um software de undervolting confiável. Alguns exemplos populares incluem o Intel Extreme Tuning Utility (XTU) para processadores Intel e o MSI Afterburner para placas gráficas NVIDIA e AMD.

3. Configuração inicial: Abra o software de undervolting e faça backup das configurações padrão ou atuais do seu componente, para que possa restaurá-las em caso de problemas.

4. Ajuste gradual: Comece por reduzir a voltagem em pequenos incrementos. Por exemplo, diminua a voltagem em 0,010 volts e teste o desempenho do sistema. Se tudo estiver a funcionar bem, continue reduzindo gradualmente.

5. Teste de estabilidade: Após cada ajuste na voltagem, é essencial testar a estabilidade do sistema. Use programas de stresse, como o Prime95 para CPU e o FurMark para GPU, para garantir que o sistema não apresente bloqueios ou falhas durante cargas intensas.

6. Monitorização: Durante o processo de undervolting e após a conclusão, monitorize regularmente as temperaturas e o desempenho do seu componente para garantir que tudo esteja a funcionar conforme o esperado.

7. Ajustes finais e otimização: Continue a ajustar a voltagem até encontrar o ponto ideal em que o componente funcione de forma estável, com temperaturas aceitáveis e consumo de energia reduzido, sem comprometer o desempenho.

8. Salvar configurações: Depois de encontrar as configurações ideais de undervolting, salve-as no software para que sejam aplicadas automaticamente sempre que o sistema for iniciado.

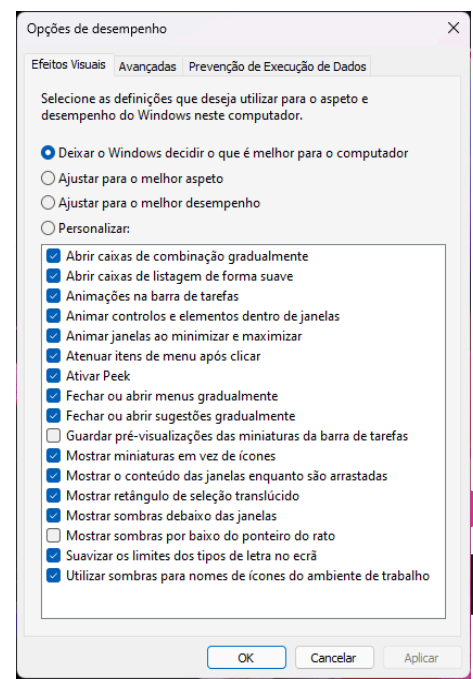
9. Monitorização contínua: Após realizar o undervolting, continue monitorizando regularmente o sistema para garantir que permanece estável e não haja problemas de desempenho ou temperatura.

Lembre-se sempre de proceder com cautela ao realizar undervolting, pois ajustes excessivos podem causar instabilidade no sistema. Se não se sentir confortável para fazer esses ajustes, é melhor procurar a ajuda de um profissional ou evitar o undervolting.

coisas desnecessárias em nome de uma aparência bonita que pode ser eliminada para gastar essa potência noutro lado.

Chegar a este menu de definições pode ser um pouco complicado. Pode abrir o menu Iniciar e começar a escrever "ajustar o aspeto e o desempenho do Windows" até que o mesmo texto apareça para selecionar, mas a pesquisa do Windows pode ser complicada. Em alternativa, pode abrir a Linha de Comandos, escrever "systempropertiesperformance.exe" e iniciar a ferramenta dessa forma.

Também pode ser encontrada em C: > Windows > System32 > SystemPropertiesPerformance.

Na ferramenta 'Opções de desempenho', selecione a guia 'Efeitos visuais' e desmarque as opções que não deseja. Quanto mais desmarcar, menos processamento extra o seu sistema irá fazer em nome de tornar o Windows bonito. Algumas destas opções são reconhecidamente muito úteis e não são susceptíveis de sobrecarregar um portátil moderadamente potente, mas se o seu sistema estiver a sofrer de lentidão considerável a cada momento,

lentas, como também a memória e o processamento que elas consomem, depois de estarem a funcionar, vão manter as coisas mais lentas até conseguir desligá-las todas.

Em vez disso, pode simplesmente impedir que todas elas sejam iniciadas. Para tal, basta ir a 'Definições' > 'Aplicações' > 'Arranque' (também pode ser rapidamente acedido escrevendo "Arranque" na barra de pesquisa do Windows e

selecionar 'Aplicações de arranque'). A partir deste menu, pode desmarcar todas as aplicações que não pretende que iniciem automaticamente sempre que o Windows arranca.

5. CERTIFIQUE-SE DE QUE NÃO HÁ PROBLEMAS DE MEMÓRIA

Mesmo que você pare a maior parte das aplicações na fase de arranque, o objetivo de ter um computador é ter coisas a correr no mesmo, então eventualmente terá que deixar alguns programas usarem os seus recursos. Mas deve estar atento aos consumidores de memória, pois são uma forma rápida de voltar a ter lentidão.

Se sentir que o seu sistema está a ficar inesperadamente lento, vá ao 'Gestor de Tarefas' (Ctrl+Shift+Esc abre-o num instante), selecione 'Processos' no menu do lado esquerdo e clique na coluna 'Memória' para a ordenar rapidamente. Aqui, poderá identificar rapidamente quaisquer programas ou processos que estejam a utilizar muita memória (ou CPU, disco ou largura de banda de rede). Se a aplicação que pretende utilizar não estiver no topo da lista, poderá haver outras aplicações que valha a pena parar.

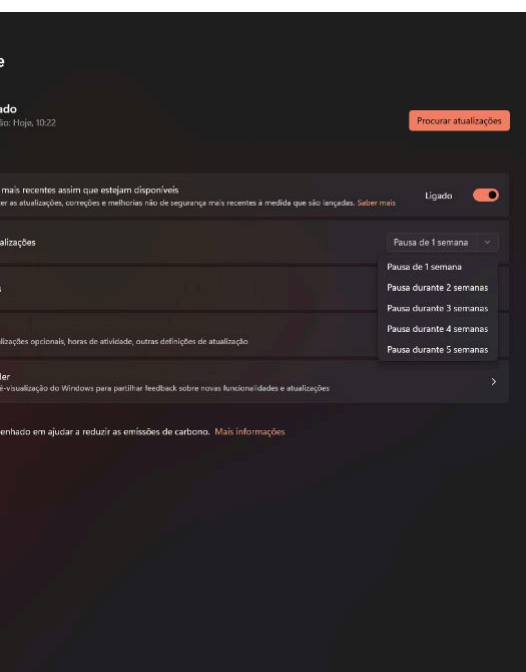
6. PAUSAR AS ATUALIZAÇÕES DO WINDOWS

Por falar em consumir muitos recursos do sistema, o Windows Update pode ser um grande problema de desempenho. O descarregamento e a instalação de atualizações podem ser bastante intensivos, e mesmo as máquinas de alto desempenho podem sentir um impacto se as atualizações estiverem a ser feitas em segundo plano.

Os sistemas de baixo desempenho são ainda mais afetados, por vezes parando sem motivo aparente até que se perceba que o Windows Update foi ativado.

A aplicação de atualizações é importante. Não se engane. Mas as atualizações podem provavelmente esperar até que você termine o que está a tentar fazer. Se aceder a 'Definições' > 'Windows Update', deverá encontrar uma opção para pausar as atualizações durante um

O Windows Update (que permite efetuar atualizações ao sistema) pode oferecer problemas de desempenho ao seu portátil

No Gestor de Tarefas poderá identificar que programas, ou processos, consomem mais memória

período de uma a cinco semanas. Pode tirar partido desta opção para ter tempo para terminar o trabalho em que está a trabalhar. Lembre-se apenas de retomar as atualizações depois disso, se quiser manter-se atualizado.

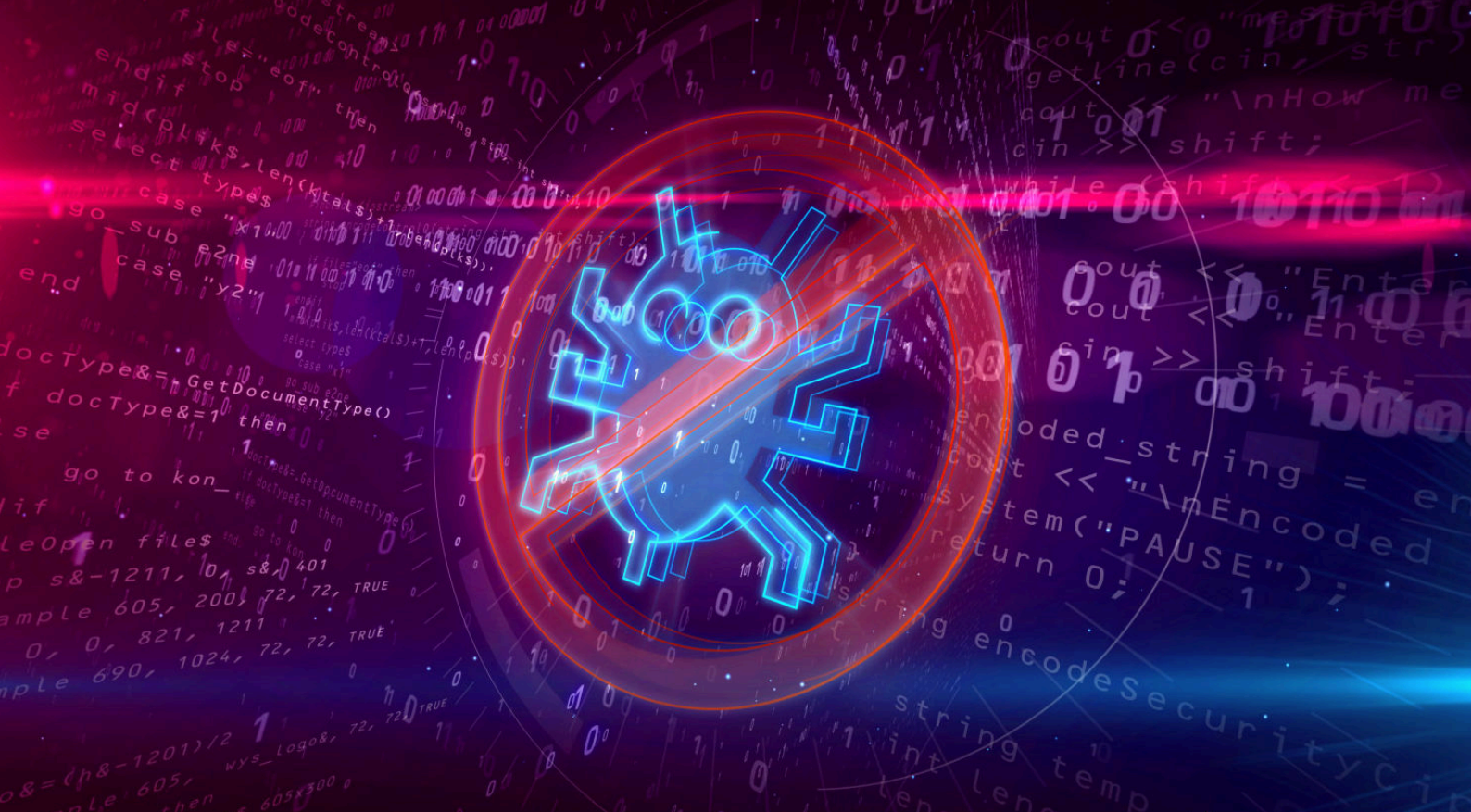
7. TIRE PARTIDO DAS DEFINIÇÕES QOS DE UM ROUTER

A velocidade do seu computador portátil não é apenas o resultado do próprio computador. Se estiver a sofrer de lentidão na Internet, a causa pode ser o seu router. Dependendo do seu router, poderá ter uma opção chamada Qualidade de Serviço (ou QoS, abreviadamente). Trata-se de uma ferramenta para dar prioridade a diferentes tráfegos e dispositivos na sua rede. Tente aceder às definições do seu router (muitas vezes, acedendo a 192.168.1.1 num browser, mas o processo varia consoante o router), encontre qualquer ferramenta de QoS que possa incluir e dê ao seu computador portátil uma prioridade mais elevada.

8. PROCURE FORMAS DE OPTIMIZAR O FLUXO DE AR

Nada abranda mais um sistema rápido do que o calor e, no caso dos computadores portáteis, é muito fácil sufocar o seu potencial. A maioria dos computadores portáteis tem um conjunto de portas e ranhuras no chassis para puxar o ar frio e expelir o ar quente. Qualquer obstrução a qualquer uma delas pode resultar na acumulação de calor e limitar o desempenho dos componentes internos do sistema. Mesmo os sistemas com refrigeração passiva, que não possuem estas aberturas, tendem a depender da transferência de calor do seu chassis metálico para o ar, pelo que também são susceptíveis de sufocar.

Para evitar isto, certifique-se de que o computador portátil não está em cima de nada macio, como um cobertor, tapete, almofada. O ideal é colocá-lo numa superfície plana onde os pés possam levantá-lo adequadamente, permitindo que o ar circule por baixo dele. Também não deve bloquear os lados ou a traseira, se tiverem saídas de ar. Pode até levar isto um pouco mais longe, colocando o portátil numa superfície com as suas próprias ranhuras ou aberturas de ventilação para restringir ainda mais o fluxo de ar. Se juntarmos a isto uma ventoinha a soprar ar fresco na direção do computador portátil, talvez consigamos um pequeno impulso.

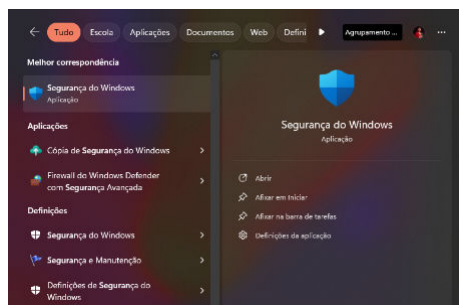
No entanto, tudo isto não terá grande significado se o seu sistema tiver aspirado tanto pó e detritos que a ventilação esteja entupida internamente. Se pensa que este pode ser o caso do seu sistema (pode ser possível ver pó no interior se o virar e olhar através da ventilação), considere abrir o portátil e limpar o pó. ■

O Windows inclui proteção integrada contra software malicioso. Eis como a ativar

O ransomware é uma coisa desagradável. Este tipo de malware encripta ficheiros no seu PC para que não lhes possa aceder, a não ser que pague ao atacante para desbloquear os dados. Por outras palavras, os seus ficheiros são mantidos reféns até que pague o resgate exigido, a menos que consiga sobreviver ao ataque de ransomware (fave.co/3Q5pUm2) utilizando outros meios.

A melhor defesa contra o ransomware é evitar sites e transferências repletos destes vírus, mas também pode tomar outras medidas de proteção. O software antivírus moderno restringe frequentemente as aplicações que podem alterar ficheiros em pastas normalmente visadas pelo ransomware. O Microsoft Defender, que está integrado no Windows, também pode fazer isso. (A Microsoft mudou o nome do Windows Defender há vários anos, mas é o mesmo programa). Alguns conjuntos de antivírus também executam cópias de segurança automáticas, caso seja necessário restaurar os seus ficheiros.

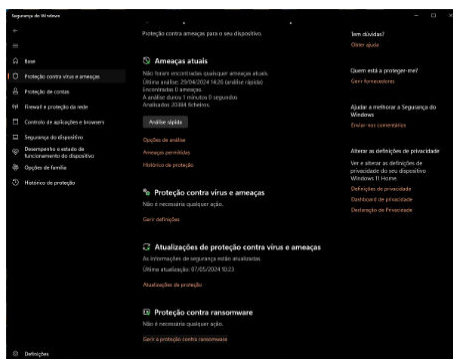
O senão? Ao contrário do software antivírus de terceiros, estas proteções extra não estão ativadas por defeito no Microsoft Defender. Tem de as ativar você mesmo.

COMO ACTIVAR A PROTECÇÃO CONTRA RANSOMWARE NO WINDOWS

PASSO 1: ABRIR O 'SEGURANÇA DO WINDOWS'
Abra a aplicação 'Segurança do Windows' no seu PC. Pode aceder a ela de várias formas:
- Prima Alt + Barra de espaços no seu teclado, escreva 'Segurança do Windows' e depois prima Enter
- Abra o menu Iniciar, escreva 'Segurança do Windows' e prima Enter
- Abra a aplicação 'Definições' e, em seguida, escolha 'Segurança do Windows' no painel esquerdo

PASSO 2: LOCALIZAR AS DEFINIÇÕES DE RANSOMWARE
Na aplicação 'Segurança do Windows', clique em 'Proteção contra vírus e ameaças'.

Depois, clique em 'Gerir proteção contra ransomware' em 'Proteção contra ransomwasre' na parte inferior do ecrã

Em seguida, ative o 'Acesso controlado a pastas'. Esta definição restringe o acesso da aplicação às pastas predefinidas OneDrive, Documentos, Imagens, Vídeos, Música e Favoritos do seu PC. Você também pode adicionar manualmente outras pastas à lista.

Nem todas as aplicações serão impedidas de aceder a estas áreas no Windows - os programas do Microsoft Office têm permissão automática para abrir e alterar ficheiros. Mas se não estiver na lista interna de aplicações de confiança da Microsoft, um programa não pode ver nada nessas pastas até que seja concedida uma permissão explícita na Segurança do Windows.

PASSO 3: CERTIFIQUE-SE DE QUE TEM SESSÃO INICIADA NO ONEDRIVE
Limitar o acesso a ficheiros e pastas não os protege completamente. Outro método de defesa importante é ter boas cópias de segurança, o que o Windows faz automaticamente se tiver sessão iniciada no OneDrive. (Pode ligar uma conta Microsoft a todo o seu PC Windows ou apenas à aplicação OneDrive especificamente).

Para confirmar que esta proteção está ativada, pode consultar 'Proteção contra ransomware' > 'Gerir a proteção contra ransomware' > 'Recuperação de dados de ransomware'.

Naturalmente, para evitar os piores efeitos do ransomware, a cópia de segurança mais segura dos seus ficheiros é aquela que mantém offline. Deve fazer uma cópia de segurança para além de tudo o que está armazenado na nuvem - se tiver apenas uma cópia dos seus dados, não está a fazer uma cópia de segurança adequada.

DEVE ATIVAR A PROTECÇÃO CONTRA RANSOMWARE NO WINDOWS?

A segurança e a comodidade vivem em extremos opostos de um espetro, e é esse o caso aqui também. O controlo do acesso a pastas no Windows pode manter os atacantes afastados das suas pastas importantes, mas também pode ser ligeiramente inconveniente. Os jogadores, por exemplo, podem descobrir que o acesso a ficheiros guardados pode estar bloqueado por predefinição, uma vez que estes são frequentemente guardados na pasta Documentos.

Pode resolver este problema com um mínimo de trabalho - adicione a aplicação à lista de acesso. Ou guarde os ficheiros do jogo numa pasta diferente no PC que não tenha acesso controlado. (Terá apenas de utilizar software de terceiros para agendar cópias de segurança regulares). ■

O que é o ransonware?

O ransomware é um tipo de malware (software malicioso) que criptografa os ficheiros ou bloqueia o acesso ao sistema de um computador ou rede, exigindo um pagamento (geralmente em criptomoedas) para descriptografar os ficheiros ou restaurar o acesso. Este tipo de ataque é uma forma de extorsão digital, onde os criminosos cibernéticos procuram lucro explorando a necessidade das vítimas de recuperar os seus dados ou acesso ao sistema. Infelizmente, o ransomware é uma ameaça séria e tem sido cada vez mais comum nos últimos anos.

LISTERY 6.3

Uma das mais eficientes ferramentas de pesquisa de ficheiros e pastas

https://tinyurl.com/mvsnax8h

O Listary 6.3 é um programa de computador extremamente útil para aumentar a produtividade dos utilizadores, especialmente para aqueles que lidam com grandes volumes de ficheiros e precisam de uma forma eficiente de encontrá-los e organizá-los. Este software é uma ferramenta de pesquisa e navegação de ficheiros para o Windows, oferecendo uma experiência integrada e intuitiva que facilita o acesso rápido a arquivos, pastas e aplicações.

FUNCIONALIDADES PRINCIPAIS

Pesquisa Rápida: O Listary 6.3 permite a busca instantânea de ficheiros e pastas no seu computador. Basta digitar parte do nome do ficheiro na barra de pesquisa e o Listary apresenta os resultados quase que instantaneamente, economizando tempo e esforço.

Integração com o Explorer: Uma das características mais apreciadas do Listary é sua integração perfeita com o Windows Explorer. Com isso, o utilizador pode aceder rapidamente a pastas frequentes e favoritas diretamente do Explorador do sistema, sem a necessidade de navegar manualmente por inúmeras subpastas.

Favoritos e Históricos: O Listary permite marcar ficheiros e pastas como favoritos, tornando-os facilmente acessíveis a partir de qualquer janela do Explorador ou janela de abrir/guardar. Além disso, mantém um histórico das pastas acedidas recentemente, permitindo uma navegação rápida por locais previamente visitados.

Comandos Personalizados: Através do Listary, pode configurar comandos personalizados para executar ações específicas, como abrir programas, pastas ou ficheiros com atalhos de teclado simples. Por exemplo, pode definir um comando para abrir o seu editor de texto favorito, ou uma pasta específica de trabalho. Isso é feito através do menu de configurações do Listary

Suporte a Aplicações de Terceiros: O Listary 6.3 suporta a integração com uma ampla gama de programas de terceiros, como Total Commander, Directory Opus e XYplorer. Essa compatibilidade aumenta ainda mais a versatilidade e utilidade do programa, permitindo que os utilizadores usem as suas ferramentas de gestão de ficheiros preferidas com o Listary.

DICAS DE USO

Uso da tecla de Atalho Global
Uma das funcionalidades mais poderosas do Listary é a tecla de atalho global (geralmente a tecla 'Win' ou 'Ctrl duas vezes'), que pode ser usada para chamar a barra de pesquisa do Listary de qualquer lugar no Windows. Isso permite ao utilizador iniciar uma pesquisa sem ter que abrir o Explorer ou qualquer outra janela.

Navegação rápida em janelas de ficheiro
Quando estiver numa janela de abrir/guardar ficheiro, basta começar a digitar o nome da pasta ou ficheiro desejado para que o Listary exiba as correspondências relevantes. Isso elimina a necessidade de navegar manualmente através das pastas para encontrar o ficheiro necessário.

Acesso rápido aos Favoritos
Os favoritos podem ser acedidos rapidamente através do atalho 'Ctrl+G' no Windows Explorer. Adicione as suas pastas mais utilizadas aos favoritos para uma navegação ainda mais eficiente.

Pesquisa avançada
A barra de pesquisa do Listary aceita operadores avançados, como 'AND', 'OR' e aspas para pesquisas exatas. Isso pode ser particularmente útil quando se lida com grandes quantidades de ficheiros e é necessário filtrar os resultados com precisão.

PRÁTICA

OS MELHORES GUIAS PASSO A PASSO

N.º 83

p26

IMPEÇA OS SEUS VIZINHOS DE UTILIZAREM O SEU WI-FI

A não ser que viva numa área remota, o seu sinal Wi-Fi irá quase de certeza entrar na casa do seu vizinho. Desde que tenha definido uma palavra-passe forte, não deve ser fácil para os vizinhos "apanharem boleia" na sua rede de banda larga - mas pode ainda ser possível. Por isso, vale a pena verificar regularmente quais os dispositivos que estão ligados ao seu router para se familiarizar com os dispositivos que devem (e não devem) estar ligados. Aqui explicamos como fazer isso e bloquear quaisquer dispositivos não autorizados para impedir que descarreguem conteúdos ou acedam a sites duvidosos através da sua ligação. Estamos a utilizar um router Huawei OptiXstar (da Vodafone), pelo que as opções no seu router podem variar ligeiramente, mas devem ser muito semelhantes.

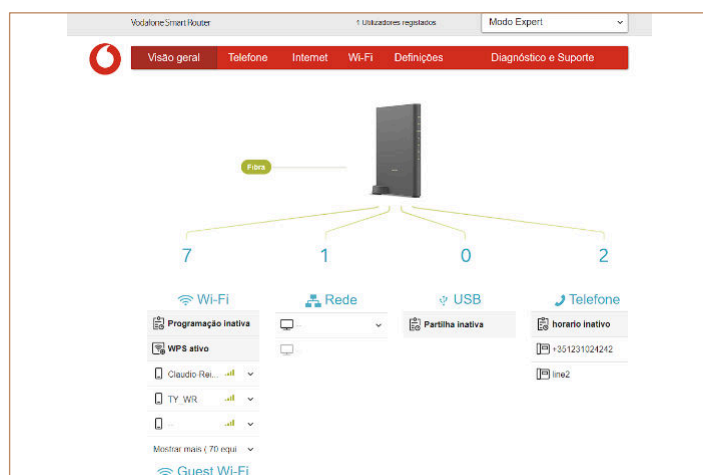
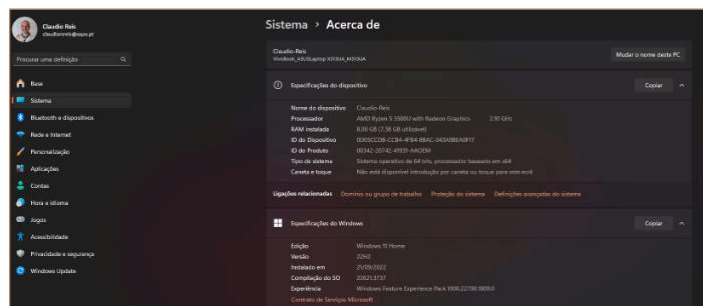
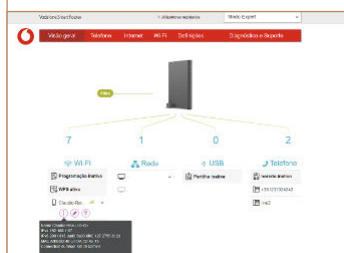
p29

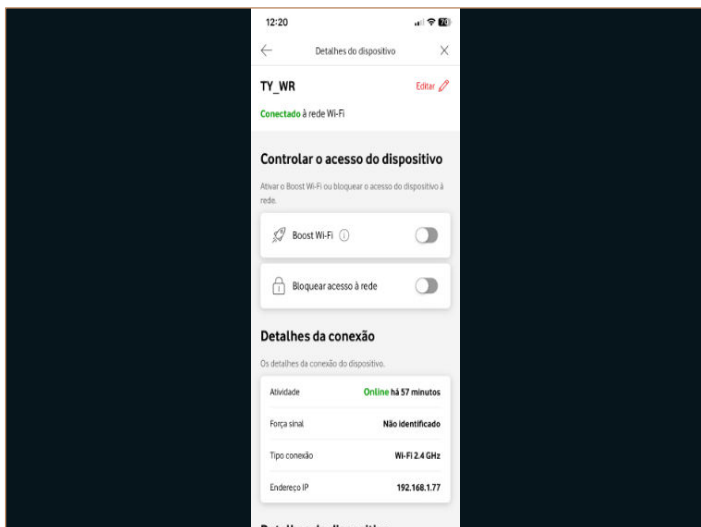
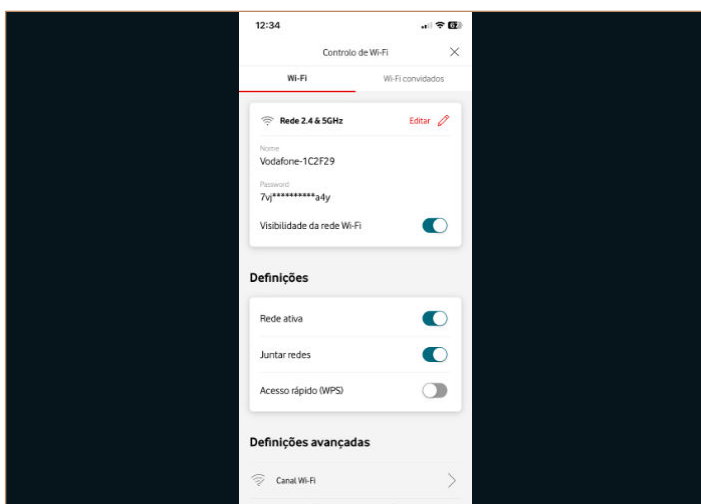
PARTILHE FICHEIROS ENTRE O SEU PC E O SEU TELEMÓVEL GRATUITAMENTE

Os serviços na nuvem, como o Google Drive e o iCloud, simplificam a tarefa de partilhar ficheiros entre o telemóvel e o computador. O problema é que, quando se partilha desta forma, é fácil acabar com ficheiros soltos a ocupar o armazenamento na nuvem depois de concluída a transferência. Isto desperdiça espaço em disco, pelo que, a não ser que faça uma limpeza, poderá um dia ter de pagar por armazenamento adicional. Em alternativa, pode utilizar o LocalSend, que, em vez de encaminhar ficheiros através da nuvem, os envia diretamente através da sua rede. É totalmente gratuito, sem restrições.

IMPEÇA OS SEUS VIZINHOS DE UTILIZAREM O SEU WI-FI

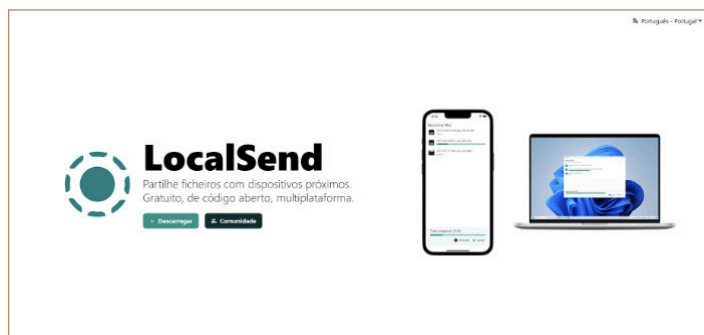
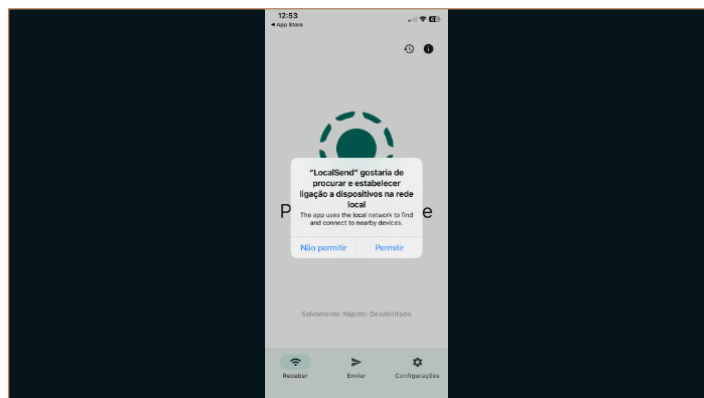
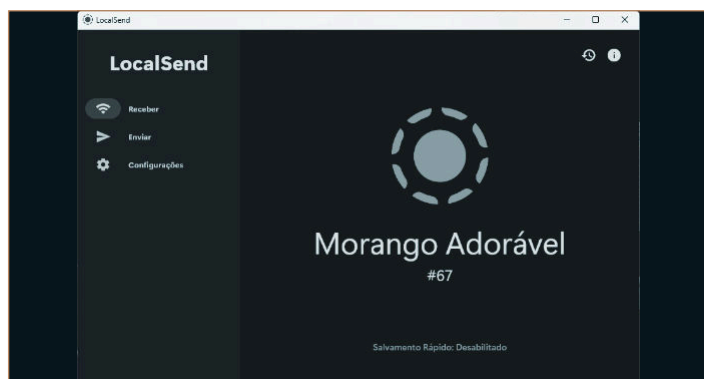
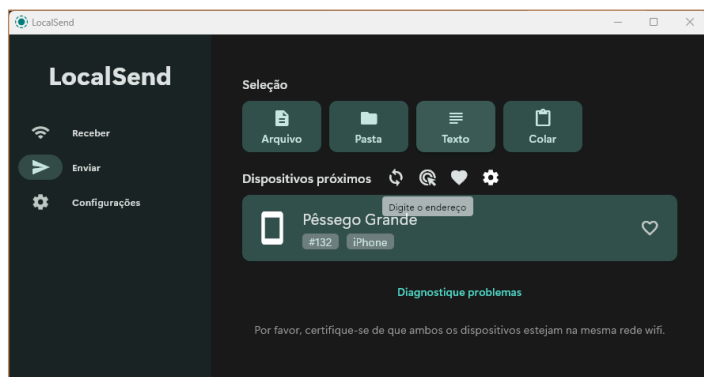
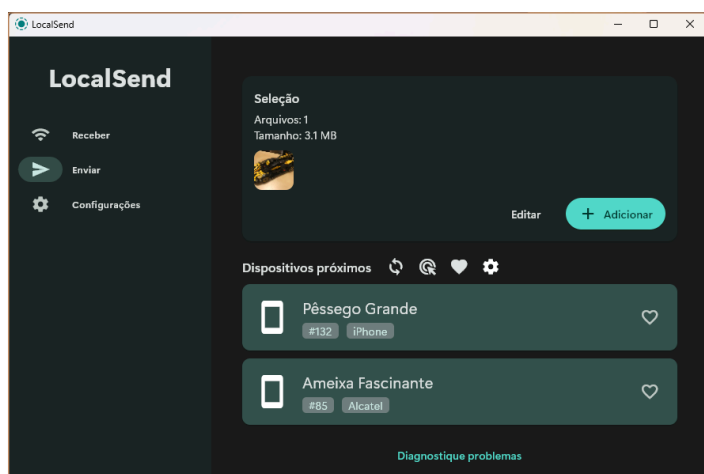
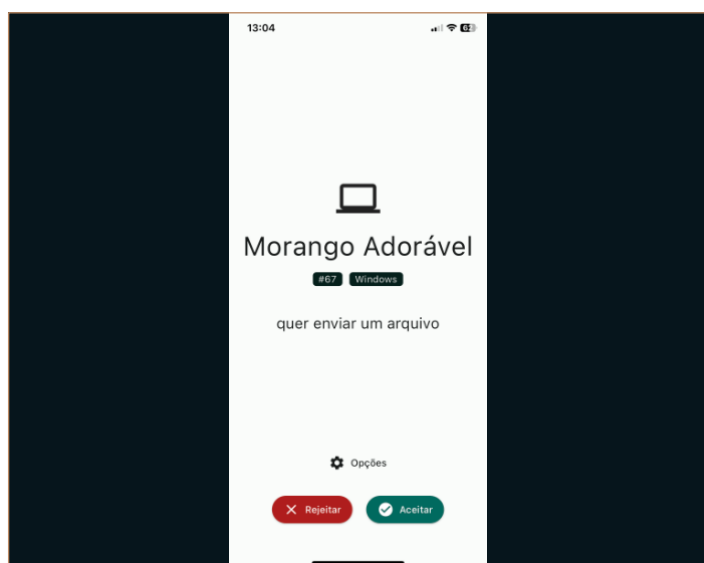
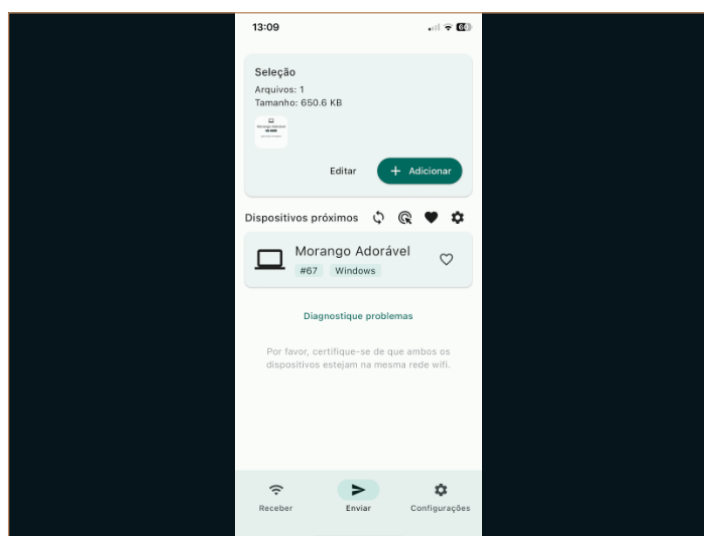
A não ser que viva numa área remota, o seu sinal Wi-Fi irá quase de certeza entrar na casa do seu vizinho. Desde que tenha definido uma palavra-passe forte, não deve ser fácil para os vizinhos "apanharem boleia" na sua rede de banda larga - mas pode ainda ser possível. Por isso, vale a pena verificar regularmente quais os dispositivos que estão ligados ao seu router para se familiarizar com os dispositivos que devem (e não devem) estar ligados. Aqui explicamos como fazer isso e bloquear quaisquer dispositivos não autorizados para impedir que descarreguem conteúdos ou acedam a sites duvidosos através da sua ligação. Estamos a utilizar um router Huawei OptiXstar (da Vodafone), pelo que as opções no seu router podem variar ligeiramente, mas devem ser muito semelhantes.

1 Abra um browser e inicie sessão no seu router. Se não souber o endereço IP pressione a tecla Windows e digite cmd e, em seguida, pressione Enter. Na janela da Linha de Comandos, digite ipconfig e pressione Enter novamente, depois procure os quatro conjuntos de dígitos ao lado de Default Gateway. Normalmente, estes serão 192.168.1.1, 192.168.1.254 ou 10.0.0.1. Escreva o endereço IP correto na barra de endereços do seu browser e, em seguida, utilize a palavra-passe de administrador da etiqueta do seu router para iniciar sessão.

2 No painel de controlo do router, procure "DHCP table" (Tabela DHCP), "Client list" (Lista de clientes), "Attached devices" (Dispositivos ligados) ou semelhante. No router que estamos a utilizar, a lista de dispositivos ligados aparece na secção 'Wi-Fi' na 'Visão geral'. Verifique a lista para ver se há algo que pareça suspeito.

3 Verifique os nomes de cada um dos computadores da sua rede para que possa fazer a correspondência com os nomes dos dispositivos na lista. Para encontrar o nome de um computador, abra as 'Definições' premindo a tecla 'Windows + I' e, em seguida, clique em 'Sistema' seguido de 'Acerca de'. O nosso computador chama-se Claudio-Reis.

4 Por vezes é impossível identificar um dispositivo pelo seu nome. Tente escrever o seu endereço num separador do browser. Na nossa rede, temos um dispositivo chamado EX3800 localizado no endereço 192.168.1.250. Digitando este endereço IP na barra de endereços do navegador, pode aparecer uma página de informações de código aberto a quem pertence esta ligação, neste caso será de um Extensor de alcance WiFi EX3800 da NetGear.

5 Se as suas investigações não conseguirem identificar um dispositivo na sua rede, tome nota do seu endereço IP e adicione-o temporariamente à lista de bloqueio do seu router. A localização da lista de bloqueio depende da marca e do modelo do seu router. No nosso caso temos de instalar a aplicação da Vodafone (Vodafone Smart Router) para poder aceder aos dispositivos que estão ligados ao router e conseguir bloquear o seu acesso à nossa rede Wi-Fi, pois via navegador não tem essa opção disponível.

6 Se reconhecer todos os dispositivos na sua rede e não tiver planos para adicionar nada de novo num futuro próximo, pode evitar ter de voltar a verificar a lista de dispositivos ligados em intervalos regulares, bloqueando todos os novos dispositivos (se o seu router o permitir). No nosso router, encontrámos uma opção identica na aplicação do telemóvel. Na secção de 'Gestão da minha rede Wi-fi'. Clique em 'Visibilidade da rede Wi-Fi' (ou semelhante) e assim a sua rede não será visível e nenhum dispositivo novo se conseguirá ligar.

7 Como é improvável que esteja a monitorizar dispositivos desonestos depois da hora de dormir, um utilizador malicioso pode tentar ligar-se apenas à noite (especialmente se estiver a utilizar a sua banda larga para descarregar filmes ou outros ficheiros grandes sem vigilância). Em alguns routers basta utilizar os controlos parentais do seu router, ou a opção de programação para desligar automaticamente o Wi-Fi pouco antes de se deitar e voltar a ligá-lo pouco antes de acordar. No nosso router acedemos a 'Wi-Fi', depois em 'Horário' e aqui definimos o horário que queremos que o router se desligue e depois volte a ligar.

PARTILHE FICHEIROS ENTRE O SEU PC E O SEU TELEMÓVEL GRATUITAMENTE

Os serviços na nuvem, como o Google Drive e o iCloud, simplificam a tarefa de partilhar ficheiros entre o telemóvel e o computador. O problema é que, quando se partilha desta forma, é fácil acabar com ficheiros soltos a ocupar o armazenamento na nuvem depois de concluída a transferência. Isto desperdiça espaço em disco, pelo que, a não ser que faça uma limpeza, poderá um dia ter de pagar por armazenamento adicional. Em alternativa, pode utilizar o LocalSend, que, em vez de encaminhar ficheiros através da nuvem, os envia diretamente através da sua rede. É totalmente gratuito, sem restrições.

1 Abra www.localsend.org e clique em 'Descarregar'. Clique em Windows no ecrã seguinte, seguido de 'EXE'. Isto descarrega uma versão do LocalSend que pode instalar. Inicie o ficheiro descarregado e clique em Instalar. Se preferir uma versão que não necessite de instalação, clique em 'Zip (Portable)', extraia os ficheiros comprimidos e, em seguida, inicie 'localsend_app. exe'. Se aparecer uma caixa a avisar que o 'Windows protegeu o seu PC', clique em 'Mais informações' seguido de 'Executar mesmo assim' para iniciar o LocalSend.

2 Descarregue a aplicação gratuita LocalSend para Android (https://tinyurl.com/3hpv73ck) ou iOS (https://tinyurl.com/2sfftp4m). Se tiver um iPhone, este pedirá autorização para encontrar dispositivos na sua rede local. Nos nossos testes, descobrimos que, embora a recusa desta opção não impeça um iPhone de receber ficheiros de um PC, impede-o de os enviar. Por isso, toque em Permitir. O Android não faz esta pergunta.

3 Com o telemóvel e o computador ligados à mesma rede sem fios, pode agora enviar ficheiros entre eles sem precisar de nomes de utilizador ou palavras-passe, ou de qualquer serviço intermediário como o Dropbox. Repare como cada dispositivo que ligou recebeu o seu próprio nome único. Como pode ver na fotografia, o iPhone, o telemóvel Android e o PC têm um nome baseado em frutas ou legumes para os podermos identificar.

4 Para enviar um ficheiro do seu PC para o seu telefone, clique em 'Enviar' e, em seguida, clique na correspondência mais próxima na secção 'Seleção' do que pretende enviar. Vamos enviar uma fotografia do nosso computador para o nosso iPhone, por isso clicamos em 'Arquivo'. Navegue até à fotografia na janela do Explorador de ficheiros que aparece, selecione-a e clique em 'Abrir'. O ficheiro substituirá o conteúdo original do painel 'Seleção', onde aparecerá um novo botão 'Adicionar'. Clique neste botão e repita o processo se pretender enviar vários ficheiros em simultâneo.

5 Clique no dispositivo para o qual pretende enviar o ficheiro selecionado. Aqui, como queremos enviar o ficheiro para o nosso iPhone, clicamos em 'Pêssego Grande'. Sabemos que isto está correto porque está marcado como um iPhone no painel 'Dispositivos próximos', enquanto o dispositivo Android está marcado como 'Ameixa Fascinante' (Alcatel). Se tivermos vários iPhones ou vários dispositivos Android, pode certificar-se de que está a enviar ficheiros para o dispositivo certo, fazendo corresponder o nome neste painel com o que é apresentado no ecrã Telefone.

6 Verifique o ecrã Telefone, onde verá um alerta de que o computador pretende enviar-lhe um ficheiro. Desde que o nome no ecrã seja igual ao nome do seu computador (para que saiba que o ficheiro vem do seu próprio PC e não de outra pessoa que utilize o LocalSend), toque em 'Aceitar'. Enquanto o nosso telemóvel Android guardou automaticamente a fotografia transferida na nossa biblioteca Fotografias, o nosso iPhone pediu permissão para a adicionar às Fotografias. Se o seu o fizer, toque em 'OK'.

7 O processo funciona da mesma forma na direção oposta. Para enviar um ficheiro de um iPhone para o PC, abra o ficheiro e, em seguida, toque no botão de partilha (um quadrado com uma seta a apontar para cima). Percorra a segunda fila de ícones, toque em LocalSend e selecione o nome da fruta ou do vegetal do seu PC como destino. No Android, abra o ficheiro que pretende enviar e toque em Partilhar. Toque em Mais na linha "Partilhar com aplicações", depois toque em LocalSend e toque no nome do seu PC. Os ficheiros são guardados na pasta Downloads (Transferências) do seu PC. Pode ainda usar a própria aplicação, tal como fez no PC. Clique em 'Enviar' depois em 'Mídia', escolha o ficheiro (permita o acesso aos ficheiros) e depois o dispositivo que o irá receber.